

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

re application of:

Shigeo TSUJII; Yasuyuki MURAKAMI; Masao KASAHARA

Serial No: not assigned

Filed: January 24, 2000

For: SECRET KEY GENERATION METHOD, ENCRYPTION
METHOD, CRYPTOGRAPHIC COMMUNICATIONS
METHOD, COMMON KEY GENERATOR,
CRYPTOGRAPHIC COMMUNICATIONS SYSTEM,
AND RECORDING MEDIAjc525 U.S. PTO
09/489696
01/24/00Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Transmitted herewith for filing is the patent application identified above.

- ☒ 5 sheet(s) of drawings (☒ formal ☐ informal) is(are) enclosed.
- ☒ 82 page(s) of specification and 1 page(s) of abstract of the invention are enclosed.
- ☒ An assignment of the invention to MURATA KIKAI KABUSHIKI KAISHA, Shigeo TSUJII and Masao KASAHARA ☒ is enclosed ☐ will follow.
- ☐ An associate power of attorney ☐ is enclosed ☐ will follow.
- ☐ A verified statement to establish small entity status under 37 C.F.R. §§ 1.9 & 1.27 is enclosed.
- ☒ Declaration and Power of Attorney ☒ is enclosed ☐ will follow.
- ☒ A certified copy of Japanese Patent Application Nos. 11-016257 filed January 25, 1999; No. 11-059049, filed March 5, 1999 from which priority is claimed under 35 U.S.C. § 119 is enclosed.
- ☐ IDS enclosed (☐ with references).
- ☐ Preliminary Amendment is enclosed.

CALCULATION OF FEES								
ITEM		TOTAL NO. OF CLAIMS		NO. OF CLAIMS OVER BASE	LG/SM \$ ENTITY FEE		\$ AMOUNT	\$ FEE
A	TOTAL CLAIMS FEE	23	-20	3	LG=\$18 SM=\$9	\$18	54	
B	INDEPENDENT CLAIMS FEE*	19	-3	16	LG=\$78 SM=\$39	\$78	1248	
C	SUBTOTAL - ADDITIONAL CLAIMS FEE (ADD FINAL COLUMN IN LINES A + B)							\$ 1302
D	MULTIPLE-DEPENDENT CLAIMS FEE					LARGE ENTITY FEE = \$260 SMALL ENTITY FEE = \$130		\$ 0
E	BASIC FEE					LARGE ENTITY FEE = \$690 SMALL ENTITY FEE = \$345		\$ 690
F	TOTAL FILING FEE (ADD TOTALS FOR LINES C, D, AND E)							\$ 1992
G	ASSIGNMENT RECORDING FEE						\$ 40	\$ 40
	*LIST INDEPENDENT CLAIMS 1, 2, 3, 4, 7, 8, 9,10,11, 12, 13, 14, 15,17,19, 20, 21, 22, 23							

- ☒ A check in the amount of \$ 1992 to cover the filing fee is enclosed.
- ☒ A check in the amount of \$ 40 to cover Assignment Recordation fee is enclosed.
- ☒ The Commissioner is hereby authorized to charge any deficiency for the following fees associated with this communication or credit any overpayment to Deposit Account No. 12-1820. **A copy of this sheet is enclosed.**
- ☒ Any additional filing fees required under 37 C.F.R. § 1.16
- ☒ Any patent application processing fees under 37 C.F.R. § 1.17

Date: January 24, 2000

Respectfully submitted,
LOEB & LOEB LLP

By: 

William H. Wright
Registration No. 36,312
Attorney for Applicant(s)

10100 Santa Monica Blvd., 22nd Floor
Los Angeles, California 90067-4164
Telephone: 310-282-2000
Facsimile: 310-282-2192

01-27-00

PATENT

Attorney Docket No: 006332-20018

A

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Shigeo TSUJII; Yasuyuki MURAKAMI; Masao KASAHARA

Serial No: not assigned

Filed: January 24, 2000

For: SECRET KEY GENERATION METHOD, ENCRYPTION
METHOD, CRYPTOGRAPHIC COMMUNICATIONS METHOD,
COMMON KEY GENERATOR, CRYPTOGRAPHIC
COMMUNICATIONS SYSTEM, AND RECORDING MEDIA

Art Unit: not assigned

Examiner: not assigned

CERTIFICATE OF MAILING VIA U.S. EXPRESS MAIL"Express Mail" Mailing Label No. EL 382 090 992 US

Date of Deposit: January 24, 2000

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

I hereby certify that

- ☒ two copies of a letter of transmittal
- ☒ check in amount of \$ 1992 as filing fee
- ☒ patent application (82 page(s) of specification; 23 claim(s); 1 page(s) of abstract
- ☒ 5 sheet(s) of formal drawings
- ☒ executed Declaration and Power of Attorney
- ☒ assignment of the invention to MURATA KIKAI KABUSHIKI KAISHA, Shigeo TSUJII and Masao KASAHARA
- ☒ certified copy of Japanese patent application No. 11-016257 filed on January 25, 1999 and 11-059049 filed March 5, 1999 from which priority is claimed in the subject case pursuant to 35 U.S.C. § 119
- ☒ return postcard

are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service with sufficient postage under 37 C.F.R. § 1.10 on the date indicated above and are addressed to:

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231.

Date: January 24, 2000

10100 Santa Monica Blvd., 22nd Floor
Los Angeles, California 90067-4164
Telephone: 310-282-2000
Facsimile: 310-282-2192

Sal Hernandez

Name of person mailing papers

Signature

KM-US-147

SECRET KEY GENERATION METHOD, ENCRYPTION METHOD,
5 CRYPTOGRAPHIC COMMUNICATIONS METHOD, COMMON KEY GENERATOR,
CRYPTOGRAPHIC COMMUNICATIONS SYSTEM, AND RECORDING MEDIA

BACKGROUND OF THE INVENTION

10

Field of the Invention

This invention relates to a secret key generation method for generating secret keys peculiar to entities, to an encryption method for encrypting information so
15 that it will be unintelligible to any but an authorized party, and to a cryptographic communications method which performs communications with ciphertext.

Description of the Related Art

20 In today's world, characterized by sophisticated information utilization, important business documents and image information are transmitted and processed in the form of electronic information over an infrastructure of computer networks. By its very nature, electronic
25 information can be easily copied, making it extremely difficult to distinguish between the copy and the

original, and information security has become a very serious problem. The realization of computer networks which support "shared computer resources," "multi-access," and "broad-area implementation" is particularly
5 indispensable to the establishment of a high-level information society. However, that very realization involves aspects which are inconsistent with the security of information exchanged between authorized parties. An effective technique for eliminating that inconsistency is
10 encryption technology, which up until now, in the course of human history, has been primarily used in the fields of military operations and foreign diplomacy.

Cryptography is the process of exchanging information so that its meaning cannot be understood by
15 anyone other than the authorized parties. In cryptographic operations, the conversion of the original text (plaintext) that anyone can understand to text (ciphertext) the meaning of which cannot be understood by a third party is called encryption, and the restoration
20 of the ciphertext to plaintext is called decryption. The overall system wherein this encryption and decryption are performed is called a cryptosystem. In the processes of encryption and decryption, respectively, secret information called encryption keys and decryption keys
25 are employed. A secret decryption key is necessary at the time of decryption, wherefore only a party

knowledgeable of that decryption key can decrypt the ciphertext. Accordingly, the confidentiality of the information is maintained by the encryption.

The encryption key and decryption key may be the same or they may be different. A cryptosystem wherein both keys are the same is called a common key cryptosystem, and the DES (Data Encryption Standards) adopted by the Bureau of Standards of the U.S. Department of Commerce is a typical example thereof. Conventional examples of such common key encryption schemes can be divided into the following three types.

(1) Type 1

Methods wherewith all common keys to be shared with possible parties in cryptographic communications are held in secret.

(2) Type 2

Methods wherewith keys are mutually shared by a preparatory communication each time cryptographic communications are conducted (including Diffie-Hellman-based key sharing scheme, key distribution scheme based on public key schemes, etc.).

(3) Type 3

Methods wherewith disclosed identification information (ID information) that specifies an individual, such as user (entity) name and address, etc., is used, and both the sending entity and receiving entity

independently generate the same common key without preparatory communications (including KPS (key predistribution systems), ID-NIKS (ID-based non-interactive key sharing schemes), etc.).

5 Such conventional methods as seen in these three types of schemes are subject to the problems described below. With method 1, since all of the common keys are stored, this scheme is unsuitable for a network society wherein an unspecified large number of users become
10 entities and conduct cryptographic communications. With method 2, there is a problem in that preparatory communications are required for key sharing.

Method 3 is a convenient method because it requires no preparatory communications, and a common key with any
15 opposite party can be generated using the disclosed ID information of the opposite party together with characteristic secret parameters distributed beforehand from a center. Nevertheless, this scheme is subject to the following two problems. Firstly, the center must
20 become a "big brother" (creating a key escrow system wherein the center holds the secrets of all of the entities). Secondly, there is a possibility that some number of entities could collude to compute the center secrets. In the face of this collusion problem, many
25 innovative techniques have been devised to circumvent the

problem by way of computation volume, but a complete solution is very difficult.

The difficulties of resolving this collusion problem arise from the fact that the secret parameters based on the ID information form dual structures comprising center secrets and personal secrets. With method 3, a cryptosystem is configured using the disclosed parameters of the center, the disclosed ID information of the individual entities, and the two types of secret parameters for the center and entities. Not only so, but it is necessary also to configure such that center secrets will not be revealed even if the entities compare the personal secrets distributed to each. Accordingly, there are many problems that must be resolved before this cryptosystem can be actually realized.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a secret key generation method, encryption method, and cryptographic communications method based on an ID-NIKS, wherewith specifying information (ID information) is divided into a plurality of portions, and all secret keys based on the divided specifying information are distributed to entities from each of a plurality of centers, whereby it is possible to minimize the

mathematical structures, circumvent the collusion problem, and facilitate the construction of the cryptosystem.

Another object of the present invention is to provide a secret key generation method, encryption method,
5 and cryptographic communications method that are more highly resistant to random number substitution attack.

According to a first aspect of the present invention, there is provided a secret key generation method for generating secret keys peculiar to entities that are to
10 be sent from a center to the entities, characterized in that the secret keys peculiar to the entities are generated using divided specifying information resulting from the division of information specifying the entities.

According to a second aspect of the present
15 invention, there is provided an encryption method wherein secret keys peculiar to entities are sent to the entities from the center respectively, and an entity encrypts plaintext to ciphertext using a secret key peculiar to that entity sent from the center, characterized in that
20 the secret keys peculiar to the entities are generated using divided specifying information resulting from the division of information specifying the entities, and plaintext is encrypted to ciphertext at one entity that
25 is a ciphertext sender using a common key generated from a component contained in its own secret key, the component corresponding to the divided specifying

information of another entity that is a destination of the ciphertext.

According to a third aspect of the present invention, there is provided a cryptographic communications method
5 for communicating information between entities, wherein one entity encrypts plaintext to ciphertext using a first common key derived from a first secret key peculiar to that entity sent from a center and sends the ciphertext to another entity (recipient), and the recipient decrypts
10 the ciphertext to the plaintext using a second common key identical to the first common key, the second common key being derived from a second secret key peculiar to the recipient sent from the center, characterized in that a plurality of the centers are deployed, each of the
15 centers generates secret keys peculiar to the entities using divided specifying information resulting from the division of information specifying the entities, and each of the entities generates the common key using a component, contained in its own secret key, corresponding
20 to the divided specifying information of an opposite entity.

The reason why the various cryptosystems based on entity specifying information proposed for the purpose of resolving the collusion problem have been unsuccessful
25 lies in excessively seeking mathematical structures to provide innovative techniques for preventing center

secrets from being deduced from entity collusion information. When the mathematical structures are too complex, the method of demonstrating safety becomes very difficult. In the present invention, therefore, the
5 mathematical structures are held to a bare minimum by dividing entity specifying information into a plurality of portions and distributing all the secret keys for each of the divided specifying information to the entities.

In the present invention, a plurality of centers are
10 deployed, and each center generates a secret key corresponding to one unit (or piece) of divided specifying information for one entity. Accordingly, no single center holds all of the entity secrets and hence no center becomes a "big brother." Also, because the
15 mathematical structures are held down to a minimum, circumvention of the collusion problem is easily realized and the cryptosystem is also simple to implement. Furthermore, the secret keys peculiar to one entity for that entity to generate a common key have been sent from
20 the centers and are stored from the start in table form, wherefore the time required for common key generation can be significantly shortened.

According to a fourth aspect of the present invention, there is provided a secret key generation
25 method for generating secret keys specific to entities using divided specifying information resulting from the

division of information specifying the entities into a plurality of blocks, characterized in that the secret key for a first block of divided specifying information has a multi-layer structure and each of the secret keys for the remaining blocks of divided specifying information has a single-layer structure.

According to a fifth aspect of the present invention, there is provided an encryption method wherein secret keys peculiar to entities are generated using divided specifying information resulting from the division of information specifying the entities into a plurality of blocks, plaintext is encrypted to ciphertext using a common key generated using a component, contained in the secret key, corresponding to the divided specifying information for an opposite entity to which the ciphertext is to be sent, characterized in that the secret key for a first block of divided specifying information has a multi-layer structure, and each of the secret keys for the remaining blocks of divided specifying information has a single-layer structure.

According to a sixth aspect of the present invention, there is provided a cryptographic communications method for communicating information between entities, wherein a plurality of centers are deployed, each of which generates secret keys peculiar to the entities using divided specifying information resulting from the

division of information specifying the entities into a plurality of blocks, one entity generates a first common key using a first component contained in secret keys peculiar to that entity sent from the centers and
5 corresponding to the divided specifying information of another entity (recipient), encrypts plaintext to ciphertext using the first common key, and sends the ciphertext to the recipient, the recipient generates a second common key identical to the first common key,
10 using a second component contained in secret keys peculiar to the recipient sent from the centers and corresponding to the divided specifying information of the ciphertext sender, and decrypts the ciphertext to the original plaintext using the second common key, the
15 secret key for a first block of divided specifying information has a multi-layer structure, and the secret keys for the remaining blocks of divided specifying information have a single-layer structure.

The present invention is configured in such a manner
20 that the common key can only be derived after the computation for all blocks is complete, and a divided block of information specifying a specific entity cannot be attacked independently, whereupon random number substitution attack can be circumvented.

25 The term "recording medium" or "computer usable (or readable) medium" in this specification includes any

physical object in which a program to be executed by CPU
or the like is stored. For example, the "recording
medium" includes a floppy disc, CD-ROM, hard disk drive,
ROM, RAM, optical recording medium such as DVD, photo-
5 magnetic recording medium such as MO, magnetic recording
medium such as magnetic tape, and semiconductor memory
such as IC card and miniature card. A data signal
embodied in a carrier wave may be the computer readable
medium.

10

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates a model diagram representing the
15 configuration of a cryptographic communications system of
the present invention;

Fig. 2 illustrates a model diagram representing an
example of entity ID vector division;

Fig. 3 illustrates a model diagram showing how
20 information is communicated between two entities;

Fig. 4 is a diagram representing the configuration
of another cryptographic communications system" according
to the present invention;

Fig. 5 depicts another example of entity ID vector
25 division;

Fig. 6 is a diagram showing how information is communicated between two entities; and

Fig. 7 is a diagram showing the configuration of a recording media.

5

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Embodiments of the present invention are now
10 described.

Fig. 1 is a model diagram representing the configuration of an cryptographic communications system of the present invention. A plurality of centers 1 (K in number) which can be trusted to maintain information
15 confidentiality are established. These centers 1 may be public institutions in a society, for example. The deployment of the plurality of centers 1 is the point of difference with the conventional third method.

These centers 1 are connected to a plurality of
20 entities a, b, ..., z that are the users employing this cryptosystem by secret channels (communication paths) 2_{a1} , 2_{aK} , 2_{b1} , ..., 2_{bK} , ..., 2_{z1} , ..., 2_{zK} . Secret information is sent from the centers 1 via these secret communication paths to the entities a, b, ..., z. Communication paths
25 3_{ab} , 3_{az} , 3_{bz} , etc., are also provided between pairs of entities. Ciphertext obtained by encrypting

communications information is sent back and forth between entities via these communication paths 3ab, 3az, 3bz, etc.

1st Embodiment:

A first embodiment that is a basic scheme of the present invention is described first.

Preparatory processing at centers 1:

The centers 1 prepare public keys and secret keys as follows and disclose the public keys.

10	Public key	P	Large prime number
		L	Size of ID vector ($L = KM$)
		K	Number of ID vector division blocks
		M	Size of divided ID vector
15	Secret key	g	GF (P) primitive element
		H_j	Symmetrical $2^M \times 2^M$ matrix formed of random numbers ($j = 1, 2, \dots, K$)
		α_{ij}	Personal secret random number of entity i (where $\alpha_{i1}\alpha_{i2} \dots \alpha_{iK} \equiv 1 \pmod{P-1}$)
20			

ID vectors that are specifying information indicating the names and addresses of entities are made L-dimension binary vectors, and each of the ID vectors is divided into K blocks (each has a block size M) as diagrammed in Fig. 2. The ID vector for entity i (i.e.

vector I_i), for example, is divided as indicated in formula 1 below. The vectors I_{ij} ($j = 1, 2, \dots, K$), that are divided specifying information, are called ID division vectors.

5

$$(1) \quad \vec{I}_i = [\vec{I}_{i1} | \vec{I}_{i2} | \dots | \vec{I}_{iK}]$$

Entity registration processing:

10

When each of the centers 1 is requested by an entity i for registration, K secret vectors s_{ij} ($j = 1, 2, \dots, K$) corresponding, respectively, to a prepared key and K ID division vectors for entity i are found according to formulas 2-1, 2-2, \dots , 2- K , as represented below, the vectors s_{ij} so found are sent to entity i in secret, and registration is complete.

15

$$(2-1) \quad \vec{s}_{i1} \equiv g^{\alpha_{i1}} H_1[\vec{I}_{i1}] \pmod{P}$$

$$(2-2) \quad \vec{s}_{i2} \equiv \alpha_{i2} H_2[\vec{I}_{i2}] \pmod{P-1}$$

20

⋮

$$(2-K) \quad \vec{s}_{iK} \equiv \alpha_{iK} H_K[\vec{I}_{iK}] \pmod{P-1}$$

25

However, when g is a scalar, and A and B are matrixes, the representation $B = g^A$ indicates that power multiplication on g is performed for each component (μ, v) of A . In other words, the result is as given in formula 3 below. The representation H_j [vector I_{ij}]

30

indicates that one row corresponding to the vector I_{ij} is extracted from the symmetrical matrix H_j , and the $[\cdot]$ operation is also defined for reference.

$$(3) \quad B_{\mu\nu} = g^{A\mu\nu}$$

Processing for generating common keys between entities:

Entity i selects from its own secret key vectors s_{i1} a vector s_{i1} [vector I_{m1}] of the component corresponding to vector I_{m1} that is the ID division vector of entity m , and also selects from among the secret key vectors s_{ij} for each of the blocks j ($j = 2, \dots, K$) the vector s_{ij} [vector I_{mj}] of the component corresponding to the vector I_{mj} . Then, entity i sequentially power-multiplies all of the vectors s_{ij} [vector I_{mj}] ($j = 2, \dots, K$) except for the vector s_{i1} [vector I_{m1}], with modulo P and the vector s_{i1} [vector I_{m1}] as the base, thereby deriving the common key K_{im} . The computation formula for finding this K_{im} specifically becomes formula 4 below. This K_{im} coincides with the common key K_{mi} derived at the entity m end.

$$\begin{aligned} (4) \quad K_{im} &\equiv \overrightarrow{s_{i1}[I_{m1}]}^{\overrightarrow{s_{i2}[I_{m2}]}} \dots \overrightarrow{s_{iK}[I_{mK}]} \\ &\equiv g^{\alpha_{i1} \dots \alpha_{iK} \cdot H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] \dots H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]} \\ &\equiv g^{H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] \dots H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]} \pmod{P} \end{aligned}$$

Next, the communication of information between entities in the cryptosystem described above is described. Fig. 3 illustrates information communicated between two entities a and b. In the example diagrammed in Fig. 3, entity a encrypts a plaintext (message) M to a ciphertext C which it sends to entity b, and entity b decrypts that ciphertext C back to the original plaintext (message) M.

A secret key generator 1a is provided at the j'th center 1 (where $j = 1, 2, \dots, K$) for deriving the vectors s_{aj} and s_{bj} (secret keys) peculiar to the entities a and b, respectively, following formula 2-j given earlier. Then, when a request for registration is tendered from the entities a and b, the secret key vectors s_{aj} and s_{bj} for those entities a and b are sent to the entities a and b.

Entity a is provided with a memory 10 for storing, in tabular form, the characteristic secret key vectors $s_{a1}, \dots, s_{aj}, \dots, s_{aK}$ sent from the K centers 1, a component selector 11 for selecting from among those secret key vectors the vector s_{a1} [vector I_{b1}], ..., vector s_{aj} [vector I_{bj}] ..., vector s_{aK} [vector I_{bK}] for the components corresponding to entity b, a common key generator 12 for generating the common key K_{ab} with entity b sought by entity a using those components selected, and an encryptor 13 for encrypting the plaintext (message) M

to the ciphertext C using that common key K_{ab} and outputting it over the communication path 30.

Entity b , meanwhile, is provided with a memory 20 for storing, in tabular form, the characteristic secret key vectors $s_{b1}, \dots, s_{bj}, \dots, s_{bK}$ sent from the centers 1, a component selector 21 for selecting from among those secret key vectors the vector s_{b1} [vector I_{a1}], \dots , vector s_{bj} [vector I_{aj}], \dots , vector s_{bK} [vector I_{aK}] for the components corresponding to entity a , a common key generator 22 for generating the common key K_{ba} with entity a sought for by entity b using those components selected, and a decryptor 23 for decrypting the ciphertext C input from the communication path 30 to the plaintext (message) M using that common key K_{ba} and outputting it.

When information is to be sent from entity a to entity b , first, the secret key vectors $s_{a1}, s_{a2}, \dots, s_{aK}$ pre-stored in the memory 10 after being derived according to the formulas 2-1, 2-2, \dots , 2- K at the centers 1 are read out to the component selector 11. Then, the component selector 11 selects the vector s_{a1} [vector I_{b1}], vector s_{a2} [vector I_{b2}], \dots , and vector s_{aK} [vector I_{bK}] that are the components corresponding to entity b , and sends them to the common key generator 12. The common key generator 12 uses these components to derive the common key K_{ab} according to formula 4, and sends that common key K_{ab} to the encryptor 13. With the encryptor 13,

this common key K_{ab} is used to encrypt the plaintext (message) M to the ciphertext C and the ciphertext C is sent via the communication path 30.

The ciphertext C sent over the communication path 30 is input to the decryptor 23 of entity b . The secret key vectors $s_{b1}, s_{b2}, \dots, s_{bK}$ derived according to formulas 2-1, 2-2, \dots , 2-K at the centers 1 and prestored in the memory 20 are read out to the component selector 21. Then, the component selector 21 selects the vector s_{b1} [vector I_{a1}], vector s_{b2} [vector I_{a2}], \dots , vector s_{bK} [vector I_{aK}] that are components corresponding to entity a , and sends them to the common key generator 22. The common key generator 22 uses these components to derive the common key K_{ba} according to formula 4 and sends this common key K_{ba} to the decryptor 23. The decryptor 23 uses the common key K_{ba} to decrypt the ciphertext C to the plaintext (message) M .

In the scheme of the present invention, the secret key vectors peculiar to the entities are stored beforehand in the memories of the entities so that a shorter time is required to generate the common keys.

The safety provided by the scheme of the present invention is now discussed.

It is known that one of the conditions necessary to a safe ID-NIKS is the inability of separating the secret key generating functions and key sharing functions in

polynomial time. A fact that the scheme of the present invention satisfies this necessary condition is described below.

Secret key generating function:

5 The scheme of the present invention has a total of K secret key generating functions as indicated in formulas 5 and 6 below.

$$\begin{aligned} (5) \quad f_1(\vec{x}) &= g^{\alpha_{i1}} H_1[\vec{x}] \quad (j=1) \\ (6) \quad f_j(\vec{x}) &= \alpha_{ij} H_j[\vec{x}] \quad (j=2, \dots, K) \end{aligned}$$

15 If H is an arbitrary symmetrical matrix, then the referencing function $[\cdot]$ is clearly indivisible, as shown in formulas 7 and 8 below.

$$\begin{aligned} (7) \quad H[\vec{x} + \vec{y}] &\neq H[\vec{x}] + H[\vec{y}] \\ (8) \quad H[\vec{x} + \vec{y}] &\neq H[\vec{x}] \cdot H[\vec{y}] \end{aligned}$$

25 Thus, the K secret key generating functions represented in formulas 5 and 6 are indivisible, as shown in formula 9 below.

$$(9) \quad f_j(\vec{x} + \vec{y}) \neq f_j(\vec{x}) \circ f_j(\vec{y}) \quad (j=1, 2, \dots, K)$$

Key sharing function:

The key sharing function in the scheme of the present invention is represented in formula 10 below.

$$(10) \quad \mathcal{F}(\vec{x}, \vec{y}) = g^{H_1[\vec{x}_1][\vec{y}_1] \cdots H_K[\vec{x}_K][\vec{y}_K]}$$

5 As in the case of the secret key generating functions, the key sharing function represented in formula 10 is indivisible, as shown in formula 11 below.

$$(11) \quad \mathcal{F}(\vec{a}, \vec{x} + \vec{y}) \neq \mathcal{F}(\vec{a}, \vec{x}) \circ \mathcal{F}(\vec{a}, \vec{y})$$

10

Attacks for breaking cryptosystems by the collusion of an indefinite number of entities (hereinafter "non-corrupting collusion") has been debated for quite some
 15 time. At the same time, attacks conducted by a smaller number of collaborators wherein only entities necessary for the attack are bought (hereinafter "corrupting collusion") are also effective if a certain individual is the only target. The safety of the scheme of the present
 20 invention against such corrupting and non-corrupting collusions is now considered.

Safety against non-corrupting collusion:

In cases where it is possible to represent the ID vector of any entity by a linear combination of
 25 collaborator ID vectors (combination attack) and either the secret key generating function or key sharing function is divisible in polynomial time, it is possible to counterfeit the secret keys of other entities from the secret keys of the collaborators (separation attack).

30 Such an attack is known as a linear attack.

In the scheme of the present invention, the ID vector of any entity can be represented as a linear combination by using the ID vectors of L collaborators who are linearly independent. That is, a combination
5 attack by L or more entities is viable. However, because the secret key generating functions and key sharing function are indivisible functions, as noted earlier, the secret key and common key of that entity cannot be counterfeited by a separation attack even in the unlikely
10 case where a combination attack against any entity should become viable. Therefore the linear attack does not work with the scheme of the present invention. Accordingly, in the face of a non-corrupting collusion, the scheme of the present invention has a collusion threshold (minimum
15 number of collaborators required for combination attack) that is far higher than L.

Safety against corrupting collusion:

In cases where an attack is made against the scheme of the present invention wherein a specific entity is
20 targeted, a random number substitution attack like that described below is conceivable wherein all of the entities required for the attack are bought out and all of the secret keys of the bought-out entities are used.

The situation is described in an example where the
25 name is four Kanji characters ($L = 4 \times 16 = 64$ bits) so that the entity ID is easy to understand and each Kanji

character is treated as 1 block. In other words, it is assumed that $K = 4$ and $M = 16$.

A case is now considered wherein the IDs of entities Z, A, B, C, and D are set as noted below, entities A, B, C, and D are bought out, and entity Z is attacked.

$$\begin{aligned}\vec{I}_Z &= [\text{辻} | \text{井} | \text{重} | \text{男}] \\ \vec{I}_A &= [\text{辻} | \text{本} | \text{恵} | \text{子}] \\ \vec{I}_B &= [\text{中} | \text{井} | \text{邦} | \text{夫}] \\ \vec{I}_C &= [\text{山} | \text{田} | \text{重} | \text{人}] \\ \vec{I}_D &= [\text{佐} | \text{藤} | \text{和} | \text{男}]\end{aligned}$$

The secret key of entity Z is then given as follows.

$$\begin{aligned}\vec{s}_{Z1} &\equiv g^{\alpha_{Z1}H_1[\text{辻}]} \pmod{P} \\ \vec{s}_{Z2} &\equiv \alpha_{Z2}H_2[\text{井}] \pmod{P-1} \\ \vec{s}_{Z3} &\equiv \alpha_{Z3}H_3[\text{重}] \pmod{P-1} \\ \vec{s}_{Z4} &\equiv \alpha_{Z4}H_4[\text{男}] \pmod{P-1}\end{aligned}$$

The collaborators make the following computations and counterfeit the secret key of entity Z.

$$\begin{aligned}\vec{s}'_{Z1} &\equiv \vec{s}_{A1} \equiv g^{\alpha_{A1}H_1[\text{辻}]} \pmod{P} \\ \vec{s}'_{Z2} &\equiv \frac{\vec{s}_{A2}[\text{井}]}{\vec{s}_{B2}[\text{本}]} \cdot \vec{s}_{B2} \equiv \frac{\alpha_{A2}H_2[\text{本}][\text{井}]}{\alpha_{B2}H_2[\text{井}][\text{本}]} \cdot \alpha_{B2}H_2[\text{井}] \\ &\equiv \alpha_{A2}H_2[\text{井}] \pmod{P-1} \\ \vec{s}'_{Z3} &\equiv \frac{\vec{s}_{A3}[\text{重}]}{\vec{s}_{C3}[\text{恵}]} \cdot \vec{s}_{C3} \equiv \frac{\alpha_{A3}H_3[\text{恵}][\text{重}]}{\alpha_{C3}H_3[\text{重}][\text{恵}]} \cdot \alpha_{C3}H_3[\text{重}] \\ &\equiv \alpha_{A3}H_3[\text{重}] \pmod{P-1}\end{aligned}$$

$$\begin{aligned}
\overrightarrow{s_{Z_4}}' &\equiv \frac{\overrightarrow{s_{A_4}[\text{男}]}}{\overrightarrow{s_{D_4}[\text{子}]}} \cdot \overrightarrow{s_{D_4}} \equiv \frac{\alpha_{A_4} H_4[\text{子}][\text{男}]}{\alpha_{D_4} H_4[\text{男}][\text{子}]} \cdot \alpha_{D_4} H_4[\text{男}] \\
&\equiv \alpha_{A_4} H_4[\text{男}] \pmod{P-1}
\end{aligned}$$

5 It may be seen here that the counterfeited vectors s_{Z_1}' to s_{Z_4}' work in the same manner as the vectors s_{Z_1} to s_{Z_4} , respectively. Hence the collusion attack is definitely viable against the scheme of the present invention in situations where it is possible to buy out
10 enough entities to mount the attack.

In order for this corrupting collusion attack to be viable, however, it is necessary to acquire the secret keys of a collaborator having exactly the same ID division vectors as the K number of ID division vectors
15 of the entity targeted for attack. For some specific block, only one entity in 2^M entities has exactly the same ID division vectors. Buying all of the K blocks for this special entity, even assuming the values $M = 10$ and $K = 100$, is hardly an easy task. Accordingly, the scheme of
20 the present invention may be said to be safe against corrupting collusions. The parameters M and K can be suitably set according to the scale of the cryptosystem and/or to the degree of safety required.

Now, in order to circumvent a random number
25 substitution attack by corrupting collusion, it is only necessary to implement measures to prevent the division

blocks from being independently attacked. In other words,
it is only necessary to make it so that the random number
terms disappear only after the computation of all of the
blocks is complete. With this perspective, two
5 embodiment are now described which represent improvements
of the first embodiment.

2nd Embodiment:

Another example of the present invention (2nd
embodiment) is now described which is made stronger
10 against random number substitution attack by combining a
random number elimination method.

Preliminary processing at centers 1:

As in the first embodiment, the centers 1 prepare
public keys and secret keys as follows and disclose the
15 public keys.

Public key	P	Large prime number
	L	Size of ID vector ($L = KM$)
	K	Number of ID vector division blocks
20	M	Size of divided ID vector
Secret key	g	GF (P) primitive element
	H_j	Symmetrical $2^M \times 2^M$ matrix formed of random numbers ($j = 1, 2, \dots, K$)
25	α_i	Personal secret random number of

entity i

(where $\alpha_{i1}\alpha_{i2} \dots \alpha_{iK} \equiv 1$

(mod $P - 1$))

In order to employ the safety of RSA ciphers, P is
5 set so that it is very difficult to factor $P - 1$ into
prime numbers. To do that it is only necessary to use a
prime number such that $P = 2pq + 1$ (where p and q are
prime).

As in the first embodiment, the ID vector of each of
10 the entities is divided into K blocks (ID division
vectors) having a block size M (cf. Fig. 2 and formula 1).

Furthermore, as indicated in formula 12 below, a
hashing function $h(\cdot)$ for generating a second ID vector v_i
of K-1 dimension from the ID is disclosed by the centers
15 1. The components of this second ID vector v_i generated
with the hashing function take positive integers, and it
is assumed that the sum thereof is a comparatively small
constant e as represented in formula 13 below.

20 (12)
$$\vec{v}_i = (v_{i2}, v_{i3}, \dots, v_{iK}) = h(ID_i)$$

(13)
$$\sum_{j=2}^K v_{ij} = e$$

25

Entity registration processing:

When the centers 1 are requested by an entity i for
registration, K secret vectors s_{ij} ($j = 1, 2, \dots, K$)

corresponding, respectively, to a prepared key and K ID division vectors for entity i are found according to formulas 14-1, 14-2, ..., 14-K, as represented below, the vectors s_{ij} so found are sent to entity i in secret, and
5 registration is complete.

$$(14-1) \quad \vec{s}_{i1} \equiv g^{\alpha_i^{-e} H_1[\vec{I}_{i1}]} \pmod{P}$$

$$10 \quad (14-2) \quad \vec{s}_{i2} \equiv \alpha_i H_2[\vec{I}_{i2}]^{v_{i2}} \pmod{P-1}$$

$$\vdots$$

$$15 \quad (14-K) \quad \vec{s}_{iK} \equiv \alpha_i H_K[\vec{I}_{iK}]^{v_{iK}} \pmod{P-1}$$

Processing for generating common key between entities:

Entity i uses the disclosed hashing function $h(\cdot)$
20 to derive the second ID vector for an opposite entity m, namely v_m , according to formula 15 below.

$$(15) \quad \vec{v}_m = (v_{m2}, v_{m3}, \dots, v_{mK}) = h(ID_m)$$

25 Entity i selects from its own secret key vectors s_{i1} a vector s_{i1} [vector I_{m1}] of the component corresponding to vector I_{m1} that is the ID division vector of entity m, and also selects from among the secret key vectors s_{ij} for the
30 blocks j ($j = 2, \dots, K$) the vector s_{ij} [vector I_{mj}] of the component corresponding to the vector I_{mj} . Then, entity i sequentially performs power-multiplications, repeatedly for v_{mj} times, on all the vectors s_{ij} [vector I_{mj}] ($j =$

2, ..., K) except for vector s_{i1} [vector I_{m1}], with modulo P and the vector s_{i1} [vector I_{m1}] as the base, thereby deriving the common key K_{im} . The computation formula for finding this K_{im} specifically becomes formula 16 below.

5 This K_{im} coincides with the common key K_{mi} obtained by the entity m .

$$\begin{aligned}
 (16) \quad K_{im} &\equiv \overrightarrow{s_{i1}}[\overrightarrow{I_{m1}}] \overrightarrow{s_{i2}}[\overrightarrow{I_{m2}}]^{v_{m2}} \dots \overrightarrow{s_{iK}}[\overrightarrow{I_{mK}}]^{v_{mK}} \\
 &\equiv g^{\alpha_i^{-e} \alpha_i^e \cdot H_1[i1][m1] \cdot H_2[i2][m2] \dots H_K[iK][mK]} \\
 &\equiv g^{H_1[i1][m1] \cdot H_2[i2][m2] \dots H_K[iK][mK]} \pmod{P}
 \end{aligned}$$

where $\overrightarrow{I_{ij}}$ is abbreviated $[ij]$ from the second equation on

Safety against random number substitution attack:

Generally, in actual examples of the aforementioned entities A and B , we will have $v_{A2} \neq v_{B2}$, so that as shown below in formula 17, the random number substitution attack is not viable.

$$\begin{aligned}
 (17) \quad \overrightarrow{s_{Z2}}' &\equiv \frac{\overrightarrow{s_{A2}}[\text{井}]}{\overrightarrow{s_{B2}}[\text{本}]} \cdot \overrightarrow{s_{B2}} \\
 &\equiv \frac{\alpha_A H_2[\text{本}][\text{井}]^{v_{A2}}}{\alpha_B H_2[\text{井}][\text{本}]^{v_{B2}}} \cdot \alpha_B H_2[\text{井}] \\
 &\neq \alpha_A H_2[\text{井}] \pmod{P-1}
 \end{aligned}$$

3rd Embodiment:

5 Another example (third embodiment) of the present invention is now described wherewith the personal random number elimination process is rendered complex by the addition of a constant term.

Preliminary processing at centers 1:

10 As in the first embodiment, the centers 1 prepare public keys and secret keys as follows and disclose the public keys.

	Public key	N	N = PQ (where P and Q are large prime numbers)
15		L	Size of ID vector (L = KM)
		K	Number of ID vector division blocks
		M	Size of divided ID vector
	Secret key	g	Maximum generating element with modulo N
20		H_j	Symmetrical $2^M \times 2^M$ matrix formed of random numbers (j = 1, 2, ..., K)
		α_{ij}	Personal secret random number of entity i
25			where $\alpha_{i1}\alpha_i \alpha_{iK} \equiv 1 \pmod{\lambda(N)}$ and $\lambda(\cdot)$ is Carmichael function

Also, as in the first embodiment, the ID vector of each entity is divided into K blocks (ID division vectors) having a block size of M (cf. Fig. 2 and formula 5 1).

Entity registration processing:

When the centers 1 are requested by an entity i for registration, K secret vectors s_{ij} ($j = 1, 2, \dots, K-1, K$) corresponding, respectively, to a prepared key and K ID division vectors for entity i are found according to formulas 18-1, 18-2, ..., 18-K-1, 18-K, as represented below.

$$(18-1) \quad \vec{s}_{i1} \equiv g^{\alpha_{i1} H_1[\vec{I}_{i1}]} \pmod{N}$$

$$(18-2) \quad \vec{s}_{i2} \equiv \alpha_i H_2[\vec{I}_{i2}] + \beta_{i2}$$

$$\vdots$$

$$(18-K-1) \quad \vec{s}_{i,K-1} \equiv \alpha_i H_{K-1}[\vec{I}_{i,K-1}] + \beta_{i,K-1}$$

$$(18-K) \quad \vec{s}_{iK} \equiv \alpha_{iK} H_K[\vec{I}_{iK}]$$

The third embodiment further adds K-2 personal random numbers $\beta_{i2}, \dots, \beta_{i,K-1}$ to the first embodiment wherein $\alpha_{i2} = \dots = \alpha_{i,K-1} = \alpha_i$ and $\alpha_{i1} \alpha_i \alpha_{iK} = 1 \pmod{\lambda(N)}$. The centers 1 derive the vectors t_i according to formula 19 below. It should be assumed here that $\beta_i = \beta_{i2} + \dots +$

$\beta_{i,K-1}$. The derived vectors s_{ij} and t_i are sent to entity i in secret and registration is complete.

$$(19) \quad \vec{t}_i \equiv g^{-\alpha_{i1} H_1[\vec{I}_{i1}]} \beta_i \pmod{N}$$

Processing for generating common key between entities:

Entity i first, from the secret key vectors s_{ij} for the blocks j ($j = 2, \dots, K-1$), selects column vectors s_{ij} [vectors I_{mj}] corresponding to the vectors I_{mj} that are the ID division vectors of entity m , block by block, and finds the sum S_{im} thereof by formula 20 below.

$$(20) \quad \begin{aligned} S_{im} &= \sum_{j=2}^{K-1} \vec{s}_{ij}[\vec{I}_{mj}] \\ &= \alpha_i \sum_{j=2}^{K-1} H_j[\vec{I}_{ij}][\vec{I}_{mj}] + \beta_i \end{aligned}$$

Entity i , from among the secret key vector s_{i1} for its own first block and the secret key vector s_{iK} for the last block, selects the column corresponding to the vectors I_{mj} that are the ID division vectors of entity m , and performs the calculation shown below in formula 21 using s_{im} and vectors t_i to derive the common key K_{im} . This K_{im} coincides with the common key K_{mi} derived by entity m .

$$(21) \quad \begin{aligned} K_{im} &\equiv \left(\vec{t}_i[\vec{I}_{m1}] \cdot \vec{s}_{i1}[\vec{I}_{m1}]^{S_{im}} \right)^{\vec{s}_{iK}[\vec{I}_{mK}]} \\ &\equiv g^{\alpha_{i1} \alpha_i \alpha_{iK} \cdot H_1[\vec{I}_{i1}][\vec{I}_{m1}] \left(\sum_{j=2}^{K-1} H_j[\vec{I}_{ij}][\vec{I}_{mj}] \right) H_K[\vec{I}_{iK}][\vec{I}_{mK}]} \end{aligned}$$

$$\equiv g^{H_1[i_1][m_1] \left(\sum_{j=2}^{K-1} H_j[i_j][m_j] \right) H_K[i_K][m_K]} \pmod{N}$$

5

→
where $[I_{ij}]$ is abbreviated $[i_j]$ from the second
equation on

10

Safety considerations:

In this formula, if settings are made as in formula
22 below, the expression $K_{im} = x_{im2} x_{im3} \dots x_{im,K-1}$ will
result, and, by gathering together numerous formulas
15 wherein $x_{im2}, x_{im3}, \dots, x_{im,K-1}$ are variables, it is
theoretically possible to counterfeit keys.

$$\begin{aligned} (22) \quad x_{im2} &= g^{H_1[i_1][m_1] H_2[i_2][m_2] H_K[i_K][m_K]} \\ x_{im3} &= g^{H_1[i_1][m_1] H_3[i_3][m_3] H_K[i_K][m_K]} \\ &\vdots \\ x_{im,K-1} &= g^{H_1[i_1][m_1] H_{K-1}[i_{K-1}][m_{K-1}] H_K[i_K][m_K]} \end{aligned}$$

20

25

However, with the scheme of the present invention,
the mathematical structures are held down to a minimum,
30 and there is no structure in their variables that is
separable, whereupon it becomes necessary to attack all
of these variables as independent variables, thus
requiring an extremely enormous number of collaborators.
Even if the final block is susceptible to elimination by
35 a random number substitution attack, the terms expressed

in formula 22 must be attacked as independent variables. Thus, in the case where $M = 10$, for example, it becomes necessary to amass 2^{20} specific equations in order to attack, so safety is enhanced.

5 Although the third embodiment pertains to a case wherein a composite number N difficult of prime factoring is used as the modulus, the same thing can of course be done in the case where $N = P$.

4th Embodiment:

10 Fig. 4 is a model diagram showing the configuration of a cryptographic communications system of the present invention. A plurality (K) of centers 1 which can be trusted to maintain information confidentiality are established. These centers 1 may be public institutions
15 in a society, for example.

These centers 1 and a plurality of entities a , b , ..., z that are users of this cryptosystem are connected by secret communication paths 2_{a1} , ..., 2_{aK} , 2_{b1} , ..., 2_{bK} , ..., 2_{z1} , ..., 2_{zK} . Thus secret key
20 information can be sent to the entities a , b , ..., z from the centers 1 via the secret communication paths. Communication paths 3_{ab} , 3_{az} , 3_{bz} , etc., are also deployed between pairs of entities so that ciphertext resulting from encrypting communications information can
25 be sent back and forth between entities via those communication paths 3_{ab} , 3_{az} , 3_{bz} , etc.

Preparatory processing at centers 1:

The centers 1 prepare public keys and secret keys as shown below, and discloses the public keys.

	Public key	N	$N = PQ$
5		K	Number of ID vector division blocks
		M_j	Size of divided ID vector (where $j = 1, 2, \dots, K$)
10		L	Size of ID vector ($L = M_1 + M_2 + \dots + M_K$)
		T	Degree of exponent portion
	Secret key	P,Q	Large prime numbers
		g	Maximum generating element with modulo N
15		H_j	Symmetrical $2^{M_j} \times 2^{M_j}$ matrix formed of random numbers
		α_i	Personal secret random number of entity i (where $\gcd(\alpha_i, \lambda(N)) = 1$ and
20			$\lambda(\cdot)$ is Carmichael function)
		β_{ij}	Personal secret random number of entity i (where $\beta_{i1} + \beta_{i2} + \dots + \beta_{iK} = \lambda(N)$)

It should be assumed that ID vectors that are specifying information indicating the names and addresses

of entities are L-dimension binary vectors, and each of their ID vectors is divided into K blocks (block sizes are M_1, M_2, \dots, M_K), as diagrammed in Fig. 5. The ID vector for entity i (i.e. vector I_i), for example, is
5 divided as indicated in formula 23 below. The vectors I_{ij} ($j = 1, 2, \dots, K$), that are divided specifying information, are called ID division vectors.

$$(23) \quad \vec{I}_i = [\vec{I}_{i1} | \vec{I}_{i2} | \dots | \vec{I}_{iK}]$$

Entity registration processing:

When the centers 1 are requested by an entity i for registration, K secret key vectors s_{ij} ($j = 1, 2, \dots, K$)
15 corresponding, respectively, to a prepared key and K ID division vectors for entity i are calculated according to formulas 24-1, 24-2, ..., 24-j, ..., 24-K below.

$$(24-1) \quad \vec{s}_{i1} = \alpha_i H_1[\vec{I}_{i1}] + \beta_{i1} \vec{1}$$

$$(24-2) \quad \begin{aligned} \vec{s}_{i2} &= \alpha_i H_2[\vec{I}_{i2}] + \beta_{i2} \vec{1} \\ &\vdots \end{aligned}$$

$$(24-j) \quad \vec{s}_{ij} = \alpha_i H_j[\vec{I}_{ij}] + \beta_{ij} \vec{1}$$

$$(24-K) \quad \begin{aligned} &\vdots \\ \vec{s}_{iK} &= \alpha_i H_K[\vec{I}_{iK}] + \beta_{iK} \vec{1} \end{aligned}$$

Vector 1 represents a vector of K dimension wherein all of the components are 1. The representation H_j
35 [vector I_{ij}] indicates a row, corresponding to the vector

I_{ij} , extracted from the symmetrical matrix H_j , and the $[\cdot]$ operation is also defined for reference.

Next, for the 1st block, $T + 1$ secret key vectors g_{it} ($t = 0, 1, 2, \dots, T$) are calculated according to 5 formulas 25-0, 25-1, 25-2, ..., 25-t, ..., 25-T below.

$$(25-0) \quad \vec{g}_{i0} \equiv g^{\alpha_i^{-T}} \vec{1} \pmod{N}$$

$$10 \quad (25-1) \quad \vec{g}_{i1} \equiv g^{\alpha_i^{-T} \vec{s}_{i1}} \pmod{N}$$

$$(25-2) \quad \vec{g}_{i2} \equiv g^{\alpha_i^{-T} \langle \vec{s}_{i1} \rangle^2} \pmod{N}$$

$$15 \quad \vdots$$

$$(25-t) \quad \vec{g}_{it} \equiv g^{\alpha_i^{-T} \langle \vec{s}_{i1} \rangle^t} \pmod{N}$$

$$20 \quad \vdots$$

$$(25-T) \quad \vec{g}_{iT} \equiv g^{\alpha_i^{-T} \langle \vec{s}_{i1} \rangle^T} \pmod{N}$$

It should be assumed that when c is a scalar and A 25 and B indicated in formulas 26 and 27 are matrixes, the expressions $B = c^A$ and $B = \langle A \rangle^c$ correspond to formulas 28 and 29, respectively.

$$30 \quad (26) \quad A = (a_{\mu\nu})$$

$$(27) \quad B = (b_{\mu\nu})$$

$$35 \quad (28) \quad b_{\mu\nu} = c^{a_{\mu\nu}}$$

$$(29) \quad b_{\mu\nu} = a_{\mu\nu}^c$$

40

One of the centers 1 sends the $T + 1$ secret key vectors g_{it} ($t = 0, 1, 2, \dots, T$) relating to 1st block to entities i in secret, while the remaining $(K - 1)$ centers 1 send $K - 1$ secret key vectors s_{ij} ($j = 2, 3, \dots, K$) relating to the blocks from the second to the last to entities i in secret.

Processing for generating common key between entities:

Entity i , for the 1st block, selects from its own $T + 1$ secret key vectors g_{it} a vector g_{it} [vector I_{m1}] of the component corresponding to vector I_{m1} that is the ID division vector of entity m . The vectors selected are represented below in formulas 30-0, 30-1, ..., 30- t , ..., 30- T .

$$\begin{aligned}
 (30-0) \quad g_{0im} &= \overrightarrow{g_{i0}}[\overrightarrow{I_{m1}}] \\
 (30-1) \quad g_{1im} &= \overrightarrow{g_{i1}}[\overrightarrow{I_{m1}}] \\
 &\vdots \\
 (30-t) \quad g_{tim} &= \overrightarrow{g_{it}}[\overrightarrow{I_{m1}}] \\
 &\vdots \\
 (30-T) \quad g_{Tim} &= \overrightarrow{g_{iT}}[\overrightarrow{I_{m1}}]
 \end{aligned}$$

Next, entity i , for the blocks 2, 3, ..., K for $j = 2, 3, \dots, K$, selects, from its own secret key vectors s_{ij} , vectors s_{ij} [vectors I_{mj}] of the components corresponding to vectors I_{mj} that are the ID division vectors of entity

m, block by block. The vectors selected are represented below in formulas 31-2, ..., 31-J, ..., 31-K.

$$(31-2) \quad x_{2im} = \overrightarrow{s_{i2}}[\overrightarrow{I_{m2}}]$$

\vdots

$$(31-j) \quad x_{jim} = \overrightarrow{s_{ij}}[\overrightarrow{I_{mj}}]$$

\vdots

$$(31-K) \quad x_{Kim} = \overrightarrow{s_{iK}}[\overrightarrow{I_{mK}}]$$

Then, the sum y_{im} for all of these is found on the integer ring as in formula 32 below.

$$(32) \quad y_{im} = \sum_{j=2}^K x_{jim}$$

And, by performing calculation as in formula 33 below, with modulo N, the common key K_{im} is derived. In the calculation in this formula 33, by completing the calculations for all of the blocks, the personal secret random number α_i is eliminated by multiplication by the inverse element thereof, and the personal secret random numbers β_{ij} , which are K in number, are eliminated by additions therefor. This K_{im} coincides with the common key K_{mi} derived by entity m.

$$\begin{aligned} (33) \quad K_{im} &\equiv \prod_{t=0}^T g_{tim}^{T C_t y_{im}^{(T-t)}} \\ &\equiv g^{\alpha_i^{-T} \sum_{t=0}^T T C_t x_{lim}^t y_{im}^{T-t}} \\ &\equiv g^{\alpha_i^{-T} (x_{lim} + y_{im})^T} \\ &\equiv g^{\alpha_i^{-T} (x_{lim} + \dots + x_{Kim})^T} \end{aligned}$$

$$\begin{aligned}
&\equiv g^{\alpha_i^{-T}(\alpha_i H_1[\vec{I}_{i1}][\vec{I}_{m1}] + \beta_{i1} + \dots + \alpha_i H_K[\vec{I}_{iK}][\vec{I}_{mK}] + \beta_{iK})^T} \\
5 \quad &\equiv g^{\alpha_i^{-T} \left\{ \alpha_i (H_1[\vec{I}_{i1}][\vec{I}_{m1}] + \dots + H_K[\vec{I}_{iK}][\vec{I}_{mK}]) + \lambda(N) \right\}^T} \\
&\equiv g^{\alpha_i^{-T} \left\{ \alpha_i (H_1[\vec{I}_{i1}][\vec{I}_{m1}] + \dots + H_K[\vec{I}_{iK}][\vec{I}_{mK}]) \right\}^T} \\
10 \quad &\equiv g^{(H_1[\vec{I}_{i1}][\vec{I}_{m1}] + \dots + H_K[\vec{I}_{iK}][\vec{I}_{mK}])^T} \pmod{N}
\end{aligned}$$

In the formula above we assumed $x_{i1m} = \text{vector } s_{i1}$ [vector I_{m1}], but this is not even known to entity i itself. Also, because T is a comparatively small number, the exponent portion can be calculated by successively and repeatedly performing power multiplication.

In the example described in the foregoing, the size M_j of the blocks may be constant for all blocks or, alternatively, some or all of the blocks may have different sizes. However, the secret key vector g_{it} is derived in relation to the 1st block, wherefore, when that size is made constant for all blocks, the secret becomes large for the 1st block. Thus, it is better to make the size of the 1st block smaller than the sizes of the other blocks. When $M_1 = 1$, in particular, the secrets distributed can be minimized and safety most enhanced.

Let us now consider the safety of the present invention against a collusive attack such as an attack against the whole cryptosystem by the collusion of a large indefinite number of entities. If the total number of entities is 1 million, then $1000000 \div 2^{20}$, wherefore M_j

= 1 and $K = 20$. If $T = 32$, then the number of exponent
 portion terms in the common key K_{im} becomes ${}_{20}H_{32} = {}_{51}C_{32} \doteq$
 4.85×10^{13} . This number of terms exceeds the total
 number of keys shared between all entities, namely ${}_{1000000}C_2$
 $\doteq 5 \times 10^{12}$. Accordingly the condition that number of
 terms > total number of shared keys is satisfied and
 safety against collusive attack is realized.

The communication of information between entities in
 the cryptosystem described in the foregoing is described
 next. Fig. 6 is a model diagram showing how information
 is communicated between two entities a and b. In the
 example diagrammed in Fig. 6, entity a encrypts a
 plaintext (message) M to the ciphertext C which it sends
 to entity b, and entity b decrypts that ciphertext C back
 to the original plaintext (message) M.

The first of the centers 1 is equipped with a secret
 key generator 1a which computes secret key vectors s_{a1} and
 s_{b1} peculiar to the entities a and b, and the secret key
 vectors g_{at} and g_{bt} ($t = 0, 1, 2, \dots, T$) numbering $T + 1$,
 according to the formulas 24-1, 25-0, ..., 25-T given
 earlier. Then, when registration requests are made by
 the entities a and b, the secret key vectors g_{at} and g_{bt}
 for those entities a and b are sent to the entities a and
 b.

The j 'th center 1 (where $j = 2, 3, \dots, K$) is equipped with a secret key generator 1a for computing the secret key vectors s_{aj} and s_{bj} peculiar to the entities a and b according to the formulas 24-2, ..., 24-K given earlier. When registration requests are made by the entities a and b, the secret key vectors s_{aj} and s_{bj} for those entities a and b are sent to the entities a and b.

Entity a is provided with a memory 10 for storing, in tabular form, the secret key vectors g_{at} ($t = 0, 1, 2, \dots, T$) and s_{aj} ($j = 2, 3, \dots, K$) sent from the centers 1, a component selector 11 for selecting from among those secret key vectors the vector g_{at} [vector I_{b1}] ($t = 0, 1, 2, \dots, T$) and the vector s_{aj} [vector I_{bj}] ($j = 2, 3, \dots, K$) for the components corresponding to entity b, a common key generator 12 for generating the common key K_{ab} with entity b derived by entity a using those components selected, and an encryptor 13 for encrypting the plaintext (message) M to the ciphertext C using the common key K_{ab} and outputting it over the channel 30.

Entity b is provided with a memory 20 for storing, in tabular form, the secret key vectors g_{bt} ($t = 0, 1, 2, \dots, T$) and s_{bj} ($j = 2, 3, \dots, K$) sent from the centers 1, a component selector 21 for selecting from among the secret key vectors the vector g_{bt} [vector I_{a1}] ($t = 0, 1, 2, \dots, T$) and the vector s_{bj} [vector I_{aj}] ($j = 2, 3, \dots, K$) for the components corresponding to entity a,

a common key generator 22 for generating the common key K_{ba} with entity a derived by entity b using those components selected, and a decryptor 23 for decrypting the ciphertext C input from the channel 30 to the plaintext M using the common key K_{ba} and outputting it.

When information is to be sent from entity a to entity b, first, the secret key vectors g_{at} ($t = 0, 1, 2, \dots, T$) and s_{aj} ($j = 2, 3, \dots, K$) pre-stored in the memory 10 after being derived at the centers 1 are read out to the component selector 11. The component selector 11 then selects the vector g_{at} [vector I_{b1}] ($t = 0, 1, 2, \dots, T$) and the vector s_{aj} [vector I_{bj}] ($j = 2, 3, \dots, K$) that are the components corresponding to entity b and sends them to the common key generator 12. The common key generator 12 uses these components to derive the common key K_{ab} according to formula 33, and sends the common key K_{ab} to the encryptor 13. The encryptor 13 utilizes this common key K_{ab} to encrypt the plaintext M to the ciphertext C and sends the ciphertext C via the channel 30.

The ciphertext C sent over the channel 30 is input to the decryptor 23 of entity b. The secret key vectors s_{bj} ($j = 2, 3, \dots, K$) and g_{bt} ($t = 0, 1, 2, \dots, T$) derived at the centers 1 and prestored in the memory 20 are read out to the component selector 21. Then, the component selector 21 selects the vector g_{bt} [vector I_{a1}]

($t = 0, 1, 2, \dots, T$) and the vector s_{bj} [vector I_{aj}] ($j = 2, 3, \dots, K$) that are components corresponding to entity a and sends them to the common key generator 22. The common key generator 22 uses these components to derive
5 the common key K_{ba} according to formula 33 and sends this common key to the decryptor 23. The decryptor 23 uses the common key K_{ba} to decrypt the ciphertext C to the plaintext M .

In the above-described example, centers are deployed
10 in a plurality, and these centers generate a plurality of keys corresponding to a plurality of units (pieces) of entity ID information respectively. In other words, each center generates a key for a certain segment of entity ID information. Therefore no single center can hold all
15 entity secrets, and the centers cannot become "big brothers." Also, the secret key vectors peculiar to the respective entities are stored beforehand in the memories of the entities, so the time required for generating common keys can be shortened.

20 Fig. 7 is a configurational diagram of an embodiment of recording media according to the present invention. The program exemplified here, which is recorded on recording media described below, comprises processes for selecting components corresponding to entity m from among
25 the secret key vectors s_{ij} and g_{it} sent to entity i from the centers and processes for finding a common key K_{im}

using those components so selected. A computer 40 is provided at each entity.

In Fig. 7, a recording medium 41 that connects the computer 40 online employs a WWW (world wide web) server computer, for example, located remotely from the site where the computer 40 is installed. A program 41a such as that described above is recorded on the recording medium 41. The program 41a read out from the recording medium 41 controls the computer 40 and thereby computes common keys at the entities for other entities to be communicated with.

A recording medium 42 provided internally in the computer 40 is a built-in hard disk drive or ROM, for example, and a program 42a as described above is recorded on the recording medium 42. The program 42a read out from the recording medium 42 controls the computer 40 and thereby computes common keys at the entities for other entities to be communicated with.

A recording medium 43 loaded in a disk drive 40a of the computer 40 is a portable optical-magnetic disk, CD-ROM, or flexible disk, etc. A program 43a such as described above is recorded on the recording medium 43. The program 43a retrieved from the recording medium 43 controls the computer 40 and thereby computes common keys at the entities for other entities to be communicated with.

With the present invention, as described in the foregoing, entity ID information is divided into a plurality of segments or pieces and a plurality of centers are established for these entity ID information pieces respectively such that each of the centers generates a particular key for a particular piece of entity ID information. Therefore, no single center can grasp all entity secrets or can become a "big brother." In addition, the mathematical structures are held down to a minimum, so that it is easy both to effectively circumvent the collusion problem and to implement the cryptosystem. Furthermore, because the entities are in possession beforehand of secret keys peculiar thereto, the time required for generating common keys can be significantly shortened.

With an ID-NIKS based on the third conventional method described earlier, in general, $L \times L$ symmetrical matrixes are center secrets, and a portion of that information is treated as a vector comprising L components and distributed to the entities. This scheme is very easy to implement but the collusion threshold is no more than approximately L . With the scheme of the present invention, on the other hand, a collusion threshold can be obtained which is far greater than L .

With the conventional scheme, by employing $2^M \times 2^M$ center secret matrixes, it is possible to configure an ID-NIKS having the same level of collusion threshold as the present invention. An ID-NIKS configured in such
5 manner is not practical, however, because it requires 2^M product computations or power-multiplication computations for key sharing. Another problem with such an ID-NIKS is that almost all schemes are divisible so that secret keys can be counterfeited for entities expressed by the linear
10 combination of some collaborators. With the scheme of the present invention, on the other hand, the number of secret keys held becomes more numerous, but the common keys can be shared by making $K-1$ power-multiplication computations, at most, key generation can be done at very
15 high speed, and, even though some entities might be expressed by the linear combination of collaborators, it is still possible to prevent the counterfeiting of secret keys for those entities.

With the present invention, moreover, the random
20 number terms are eliminated only after all blocks have been completely computed, wherefore divided blocks cannot be independently attacked and it is possible to circumvent random number substitution attack.

The above illustrated and described secret key
25 generation method, encryption method, cryptographic communications method, common key generator,

cryptographic communications system, and recording media
are disclosed in Japanese Patent Application Nos. 11-
16257 and 11-59049 filed on January 25, 1999 and March 5,
1999 respectively, the instant application claims
5 priority of these Japanese Applications, and the entire
disclosure thereof is herein incorporated by reference.

C L A I M S

What Is Claimed Is:

5

1. A secret key generation method for generating secret keys to be sent from a center to entities, comprising the step of:

generating said secret keys peculiar to said
10 entities using pieces of information resulting from division of information specifying each of said entities.

2. An encryption method for use in a system in which a center sends to entities secret keys peculiar to
15 the entities respectively, and each entity uses a secret key peculiar to itself that has been sent from the center when it encrypts plaintext to ciphertext, the encryption method comprising the steps of:

generating said secret keys peculiar to said
20 entities using pieces of information resulting from division of information specifying each of said entities;
and

encrypting plaintext to ciphertext using a common key generated using a component contained in the secret
25 key peculiar to an entity that is a sender of the ciphertext, the component corresponding to one or more

pieces of information specifying another entity that is a destination of the ciphertext.

3. A cryptographic communications method for
5 communications of information between entities wherein a plurality of centers are provided, each of which generates secret keys peculiar to the entities using divided pieces of information resulting from division of information specifying each of the entities; one entity
10 generates a first common key using a first component contained in secret keys peculiar to the one entity sent from the centers, encrypts plaintext to ciphertext using the first common key and sends the ciphertext to another entity, the first component corresponding to one or more
15 of the divided pieces of information specifying said another entity; and said another entity generates a second common key identical to the first common key using a second component contained in secret keys peculiar to the another entity sent from said centers, and decrypts
20 said ciphertext to the original plaintext using the second common key, the second component corresponding to one or more of the divided pieces of information specifying the one entity.

25 4. A cryptographic communications method for communicating information between entities wherein:

secret keys peculiar to said entities are sent from
a center to said entities;

one entity encrypts plaintext to ciphertext using a
first common key derived from a first secret key peculiar
5 to the one entity sent from said center and sends the
ciphertext to another entity;

said another entity decrypts said ciphertext to the
original plaintext using a second common key identical to
the first common key, the second common key being derived
10 from a second secret key peculiar to said another entity
sent from said center, characterized in that;

a plurality of said centers are deployed;

each of said plurality of centers generates secret
keys peculiar to said entities by adding random numbers
15 peculiar to said entities to divided pieces of
information resulting from division of information
specifying each of said entities; and

each of said entities generates a common key using a
component, contained in the secret key peculiar to that
20 selfsame entity, corresponding to one or more of the
divided pieces of information specifying an opposite
entity.

5. The cryptographic communications method
25 according to claim 4, wherein computation formulas for
generating secret keys at said centers are as follows:

$$\vec{S}_{i1} \equiv g^{\alpha_{i1} H_1} [\vec{I}_{i1}] \pmod{P}$$

$$\vec{S}_{i2} \equiv \alpha_{i2} H_2 [\vec{I}_{i2}] \pmod{P-1}$$

$$\vec{S}_{iK} \equiv \alpha_{iK} H_K [\vec{I}_{iK}] \pmod{P-1}$$

where

vector s_{ij} is a secret key corresponding to j 'th
piece of divided information specifying
entity i ($j = 1, 2, \dots, K$)

[vector I_{ij}] is j 'th piece of divided information
specifying entity i ;

P is a prime number;

K is number of divisions in the information
specifying entity i ;

g is primitive element for $GF(P)$;

H_j is a symmetrical $2^M \times 2^M$ matrix made up of
random numbers;

M is size of divisions in the information
specifying entity i ; and

α_{ij} is a personal secret random number for
entity i (where $\alpha_{i1} \dots \alpha_{iK} \equiv 1 \pmod{P-1}$).

6. The cryptographic communications method
according to claim 5, wherein computation formulas for
generating common keys at said entities are as follows:

$$\begin{aligned}
K_{im} &\equiv \overrightarrow{S_{i1}} [\overrightarrow{I_{m1}}] \overrightarrow{S_{i2}} [\overrightarrow{I_{m2}}] \dots \overrightarrow{S_{iK}} [\overrightarrow{I_{mK}}] \\
&\equiv \overrightarrow{g} \overrightarrow{\alpha_{i1}} \dots \overrightarrow{\alpha_{iK}} H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] \dots H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}] \\
&\equiv \overrightarrow{g} H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] \dots H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}] \pmod{P}
\end{aligned}$$

where

- 5 K_{im} is common key generated by one entity i for another entity m ; and
- vector s_{ij} [vector I_{ij}] is a component contained in secret key vector s_{ij} of entity i , corresponding to divided piece of
- 10 information specifying entity m .

7. A common key generator provided at entities in a cryptographic communications system for generating common keys to be used in processing to encrypt plaintext

15 into ciphertext and in processing to decrypt ciphertext into plaintext, comprising:

storage means at each entity for storing secret keys peculiar to each respective entity produced for respective pieces of information resulting from division

20 of information specifying each of said respective entities;

selection means for selecting components corresponding to pieces of information specifying opposite entities to be communicated with, from among the

25 secret keys stored; and

means for generating said common keys using said components so selected.

8. A cryptographic communications system for
5 reciprocally performing, between a plurality of entities, encrypting processing for encrypting plaintext that is information to be sent into ciphertext and decrypting processing for decrypting ciphertext so sent back into original plaintext; comprising:

10 a plurality of centers that generate secret keys peculiar to said entities using pieces of information resulting from division of information specifying each of said entities and that sends said secret keys to said entities; and

15 a plurality of entities each of which generates a common key employed mutually in said encryption and decryption processing when communicating with another entity, using a component contained in own secret key sent from the centers, the component corresponding to one
20 or more pieces of information specifying said another entity.

9. A computer readable recording medium that stores a program that generates at entities involved in
25 communications common keys used in processing to encrypt plaintext to ciphertext and in processing to decrypt said

ciphertext to said plaintext in a cryptographic communications system, comprising:

first program code means for causing said computer to select a component corresponding to one or more of
5 divided pieces of information specifying one entity from a secret key peculiar to another entity; and

second program code means for causing said computer to generate said common keys using said components selected.

10

10. An encryption method comprising the steps of:

generating a first secret key peculiar to ciphertext sending entity using first divided specifying information and a second secret key peculiar to ciphertext receiving
15 entity using second divided specifying information, the first divided specifying information being obtained by dividing specifying information of the ciphertext sending entity into a plurality of blocks and the second divided specifying information being obtained by dividing
20 specifying information of the ciphertext receiving entity into a plurality of blocks;

generating a common key using a component contained in the first secret key, the component corresponding to second divided specifying information of the ciphertext
25 receiving entity, the common key having a structure of at

least three layers and an exponent portion of the common key having a multi-layer structure; and

encrypting plaintext to ciphertext using the common key.

5

11. A secret key generation method comprising the step of:

generating secret keys peculiar to entities using divided specifying information resulting from division of
10 information specifying said entities into a plurality of blocks; and wherein

secret key for a first block of divided specifying information has a multi-layer structure; and

each of secret keys for remaining blocks of divided
15 specifying information has a single-layer structure.

12. An encryption method comprising the steps of:

generating secret keys peculiar to entities using divided specifying information resulting from division of
20 information specifying said entities into a plurality of blocks; and

encrypting plaintext to ciphertext at one entity using a common key generated using a component contained in the secret key peculiar to the one entity, the
25 component corresponding to divided specifying information

for another entity to which said ciphertext is to be sent,
and wherein

secret key for first block of divided specifying
information has a multi-layer structure; and

5 each of secret keys for remaining blocks of divided
specifying information has a single-layer structure.

13. A cryptographic communications method for
communications of information between entities wherein a
10 plurality of centers are provided, each of which
generates secret keys peculiar to the entities using
divided specifying information resulting from division of
information specifying each of the entities into a
plurality of blocks; one entity generates a first common
15 key using a first component contained in secret keys
peculiar to the one entity sent from the centers,
encrypts plaintext to ciphertext using the first common
key and sends the ciphertext to another entity, the first
component corresponding to one or more of the divided
20 pieces of information specifying said another entity; and
said another entity generates a second common key
identical to the first common key using a second
component contained in secret keys peculiar to the
another entity sent from said centers, and decrypts said
25 ciphertext to the original plaintext using the second
common key, the second component corresponding to one or

more of the divided pieces of information specifying the one entity; secret keys for first block of divided specifying information have a multi-layer structure; and secret keys for remaining blocks of divided specifying
5 information have a single-layer structure.

14. A secret key generation method for generating secret keys peculiar to entities using divided specifying information resulting from division of information
10 specifying said entities into a plurality of blocks, wherein:

computation formulas for generating said secret keys are as follows:

$$\begin{aligned}
 \vec{S}_{i1} &= \alpha_i H_1[\vec{I}_{i1}] + \beta_{i1} \vec{1} \\
 \vec{S}_{i2} &= \alpha_i H_2[\vec{I}_{i2}] + \beta_{i2} \vec{1} \\
 &\vdots \\
 \vec{S}_{ij} &= \alpha_i H_j[\vec{I}_{ij}] + \beta_{ij} \vec{1} \\
 &\vdots \\
 \vec{S}_{iK} &= \alpha_i H_K[\vec{I}_{iK}] + \beta_{iK} \vec{1} \\
 \\
 \vec{g}_{i0} &\equiv g^{\alpha_i^{-T}} \vec{1} \pmod{N} \\
 \vec{g}_{i1} &\equiv g^{\alpha_i^{-T}} \vec{S}_{i1} \pmod{N} \\
 \vec{g}_{i2} &\equiv g^{\alpha_i^{-T}} \langle \vec{S}_{i1} \rangle^2 \pmod{N} \\
 &\vdots \\
 \vec{g}_{it} &\equiv g^{\alpha_i^{-T}} \langle \vec{S}_{i1} \rangle^t \pmod{N} \\
 &\vdots \\
 \vec{g}_{iT} &\equiv g^{\alpha_i^{-T}} \langle \vec{S}_{i1} \rangle^T \pmod{N}
 \end{aligned}$$

where

vector s_{ij} is a secret key corresponding to j 'th

divided specifying information for entity
 i ($j = 1, 2, \dots, K$)
[vector I_{ij}] is j 'th divided specifying
information for entity i ;

5 vector 1 is a vector of dimension K wherein all
components are 1 ;

H_j is a symmetrical $2^{M_j} \times 2^{M_j}$ matrix made up of
random numbers;

M_j is size of j 'th divided specifying
10 information for entity i ;

K is number of block divisions in information
specifying entity i ;

α_i is a personal secret random number for entity
 i (where $\gcd(\alpha_i, \lambda(N)) = 1$ and $\lambda(\cdot)$ is
15 Carmichael function);

N is such that $N = PQ$ (where P and Q are
prime);

β_{ij} is a personal secret random number for
entity i (where $\beta_{i1} + \beta_{i2} + \dots + \beta_{iK} =$
20 $\lambda(N)$);

g is maximum generating element with modulo N ;
vector g_{it} is a secret key for 1st block of
specifying information for entity i ($t = 0,$
 $1, 2, \dots, T$);

25 T is degree of exponent portion; and

if c is a scalar, and A and B are matrixes represented in (i) and (ii) below, then the expressions $B = c^A$ and $B = \langle A \rangle^c$ represent (iii) and (iv) below, respectively.

5

$$(i) \quad A = (a_{\mu\nu})$$

$$(ii) \quad B = (b_{\mu\nu})$$

10

$$(iii) \quad b_{\mu\nu} = c^{a_{\mu\nu}}$$

$$(iv) \quad b_{\mu\nu} = a_{\mu\nu}^c$$

15

15. An encryption method wherein:

secret keys peculiar to entities are generated using divided specifying information resulting from division of information specifying each of said entities into a plurality of blocks;

20

plaintext is encrypted to ciphertext at one entity using a common key generated using a component contained in the secret key peculiar to the one entity, the component corresponding to divided specifying information for another entity that is a destination of said

25

ciphertext; and

computation formulas for generating said secret keys peculiar to said entities are as follows:

$$\overrightarrow{S_{i1}} = \alpha_i H_1[\overrightarrow{I_{i1}}] + \beta_{i1} \overrightarrow{1}$$

$$\overrightarrow{S_{i2}} = \alpha_i H_2[\overrightarrow{I_{i2}}] + \beta_{i2} \overrightarrow{1}$$

⋮

$$\vec{S}_{ij} = \alpha_i H_j [\vec{I}_{ij}] + \beta_{ij} \vec{1}$$

$$\vec{S}_{iK} = \alpha_i H_K [\vec{I}_{iK}] + \beta_{iK} \vec{1}$$

$$\vec{g}_{i0} \equiv g^{\alpha_i^{-T}} \vec{1} \pmod{N}$$

$$\vec{g}_{i1} \equiv g^{\alpha_i^{-T}} \vec{S}_{i1} \pmod{N}$$

$$5 \quad \vec{g}_{i2} \equiv g^{\alpha_i^{-T}} \langle \vec{S}_{i1} \rangle^2 \pmod{N}$$

$$\vec{g}_{it} \equiv g^{\alpha_i^{-T}} \langle \vec{S}_{i1} \rangle^t \pmod{N}$$

$$\vec{g}_{iT} \equiv g^{\alpha_i^{-T}} \langle \vec{S}_{i1} \rangle^T \pmod{N}$$

where

10 vector s_{ij} is a secret key corresponding to j 'th
divided specifying information for entity
 i ($j = 1, 2, \dots, K$)

[vector I_{ij}] is j 'th divided specifying
information for entity i ;

15 vector 1 is a vector of dimension K wherein all
components are 1;

H_j is a symmetrical $2^{M_j} \times 2^{M_j}$ matrix made up of
random numbers;

20 M_j is size of j 'th divided specifying
information for entity i ;

K is number of block divisions in information
specifying entity i ;

α_i is a personal secret random number for entity
 i

25 (where $\gcd(\alpha_i, \lambda(N)) = 1$ and $\lambda(\cdot)$ is

Carmichael function);

N is such that $N = PQ$ (where P and Q are prime);

β_{ij} is a personal secret random number for entity i

(where $\beta_{i1} + \beta_{i2} + \dots + \beta_{iK} = \lambda(N)$);

g is maximum generating element with modulo N;

vector g_{it} is a secret key for 1st block of specifying information for entity i ($t = 0, 1, 2, \dots, T$);

T is degree of exponent portion; and

if c is a scalar, and A and B are matrixes represented in (i) and (ii) below, the

expressions $B = c^A$ and $B = \langle A \rangle^c$ represent (iii) and (iv) below, respectively.

$$(i) \quad A = (a_{\mu\nu})$$

$$(ii) \quad B = (b_{\mu\nu})$$

$$(iii) \quad b_{\mu\nu} = c^{a_{\mu\nu}}$$

$$(iv) \quad b_{\mu\nu} = a_{\mu\nu}^c$$

16. The encryption method according to claim 15, wherein computation formulas for generating said common keys are as follows:

$$g_{0im} = \overrightarrow{g_{i0}} [\overrightarrow{I_{m1}}]$$

$$\begin{aligned}
g_{1im} &= \overrightarrow{g_{i1}} [I_{m1}] \\
g_{tim} &= \overrightarrow{g_{it}} [I_{m1}] \\
g_{Tim} &= \overrightarrow{g_{iT}} [I_{m1}] \\
x_{2im} &= \overrightarrow{s_{i2}} [I_{m2}] \\
x_{jim} &= \overrightarrow{s_{ij}} [I_{mj}] \\
x_{Kim} &= \overrightarrow{s_{iK}} [I_{mK}]
\end{aligned}$$

5

$$\begin{aligned}
K_{im} &\equiv \prod_{t=0}^T g_{tim}^{T C_t y_{im}^{(T-t)}} \\
&\equiv g_{i1}^{-T} \sum_{t=0}^T C x_{1im}^t y_{im}^{T-t} \\
&\equiv g_{i1}^{-T} (x_{1im} + y_{im})^T \\
&\equiv g_{i1}^{-T} (x_{1im} + \dots + x_{kim})^T \\
&\equiv g_{i1}^{-T} (\alpha_i H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \beta_{i1} + \dots + \alpha_i H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}] + \beta_{iK})^T \\
&\equiv g_{i1}^{-T} (\alpha_i (H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \dots + H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}]) + \lambda \mathbb{O})^T \\
&\equiv g_{i1}^{-T} (\alpha_i (H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \dots + H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}]))^T \\
&\equiv g_{i1}^{-T} (H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \dots + H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}])^T \pmod{N}
\end{aligned}$$

10

15

where

g_{tim} (= vector g_{it} [vector I_{m1}]) is a component corresponding to vector I_{m1} for entity m , selected from own vector g_{it} for 1st block of information specifying entity i ($t = 0, 1, 2, \dots, T$);

20

$x_{1im} = \text{vector } s_{i1} [\text{vector } I_{m1}];$

x_{jim} (= vector s_{ij} [vector I_{mj}]) is a component corresponding to vector I_{mj} for entity m , selected from own vector s_{ij} for j 'th block of information specifying entity i ($j = 2, 3, \dots, K$);

25

K_{im} is a common key generated by one entity i
for another entity m ; and

y_{im} is sum of $(K-1)$ components x_{jim} ($j = 2, 3,$
..., K), that is, $y_{im} = x_{2im} + x_{3im} + \dots +$

5 $x_{Kim}.$

17. A cryptographic communications method for
communications of information between entities, wherein

a plurality of centers are deployed, each of which
10 generates secret keys peculiar to said entities using
divided specifying information resulting from division of
information specifying each of said entities into a
plurality of blocks, and sends the secret keys to the
entities respectively;

15 one entity generates a first common key using a
first component contained in secret keys peculiar to the
one entity sent from the centers, encrypts plaintext to
ciphertext using the first common key, and sends the
ciphertext to said another entity, the first component
20 corresponding to divided specifying information for
another entity;

said another entity generates a second common key
identical to the first common key using a second
component contained in secret keys peculiar to said
25 another entity sent from the centers, and decrypts said
ciphertext using the second common key, the second

component corresponding to divided specifying information for the one entity; and

computation formulas for generating said secret keys at said centers are as follows:

$$\begin{aligned}
 \vec{S}_{i1} &= \alpha_i H_1 [\vec{I}_{i1}] + \beta_{i1} \vec{1} \\
 \vec{S}_{i2} &= \alpha_i H_2 [\vec{I}_{i2}] + \beta_{i2} \vec{1} \\
 \vdots \\
 \vec{S}_{ij} &= \alpha_i H_j [\vec{I}_{ij}] + \beta_{ij} \vec{1} \\
 \vdots \\
 \vec{S}_{iK} &= \alpha_i H_K [\vec{I}_{iK}] + \beta_{iK} \vec{1}
 \end{aligned}$$

$$\begin{aligned}
 \vec{g}_{i0} &\equiv g \alpha_i^{-T} \vec{1} \pmod{N} \\
 \vec{g}_{i1} &\equiv g \alpha_i^{-T} \vec{S}_{i1} \pmod{N} \\
 \vec{g}_{i2} &\equiv g \alpha_i^{-T} \langle \vec{S}_{i1} \rangle^2 \pmod{N} \\
 \vdots \\
 \vec{g}_{it} &\equiv g \alpha_i^{-T} \langle \vec{S}_{i1} \rangle^t \pmod{N} \\
 \vdots \\
 \vec{g}_{iT} &\equiv g \alpha_i^{-T} \langle \vec{S}_{i1} \rangle^T \pmod{N}
 \end{aligned}$$

where

vector s_{ij} is a secret key corresponding to j 'th divided specifying information for entity i ($j = 1, 2, \dots, K$)

$[\text{vector } I_{ij}]$ is j 'th divided specifying information for entity i ;

vector $\vec{1}$ is a vector of dimension K wherein all components are 1;

H_j is a symmetrical $2^{M_j} \times 2^{M_j}$ matrix made up of random numbers;

M_j is size of j 'th divided specifying

information for entity i ;

K is number of block divisions in information
specifying entity i ;

5 α_i is a personal secret random number for entity
 i (where $\gcd(\alpha_i, \lambda(N)) = 1$ and $\lambda(\cdot)$ is
Carmichael function);

N is such that $N = PQ$ (where P and Q are
prime);

10 β_{ij} is a personal secret random number for
entity i (where $\beta_{i1} + \beta_{i2} + \dots + \beta_{iK} =$
 $\lambda(N)$);

g is maximum generating element with modulo N ;
vector g_{it} is a secret key for 1st block of

15 information specifying entity i ($t = 0,$
 $1, 2, \dots, T$);

T is degree of exponent portion; and

if c is a scalar, and A and B are matrixes

represented in (i) and (ii) below, the

20 expressions $B = c^A$ and $B = \langle A \rangle^c$ represent
(iii) and (iv) below, respectively.

(i) $A = (a_{\mu\nu})$

25 (ii) $B = (b_{\mu\nu})$

(iii) $b_{\mu\nu} = c^{a_{\mu\nu}}$

(iv) $b_{\mu\nu} = a_{\mu\nu}^c$

18. The cryptographic communications method according to claim 17, wherein computation formulas for generating said common keys are as follows:

$$\begin{aligned}
 &g_{0im} = \overrightarrow{g_{i0}} [\overrightarrow{I_{m1}}] \\
 &g_{1im} = \overrightarrow{g_{i1}} [\overrightarrow{I_{m1}}] \\
 &\vdots \\
 &g_{tim} = \overrightarrow{g_{it}} [\overrightarrow{I_{m1}}] \\
 &\vdots \\
 &g_{Tim} = \overrightarrow{g_{iT}} [\overrightarrow{I_{m1}}] \\
 &x_{2im} = \overrightarrow{s_{i2}} [\overrightarrow{I_{m2}}] \\
 &\vdots \\
 &x_{jim} = \overrightarrow{s_{ij}} [\overrightarrow{I_{mj}}] \\
 &\vdots \\
 &x_{Kim} = \overrightarrow{s_{iK}} [\overrightarrow{I_{mK}}] \\
 \\
 &K_{im} \equiv \prod_{t=0}^T g_{tim}^{C_t y_{im}^{(T-t)}} \\
 &\equiv g_{i1}^{-T} \sum_{t=0}^T C_t x_{1im}^t y_{im}^{T-t} \\
 &\equiv g_{i1}^{-T} (x_{1im} + y_{im})^T \\
 &\equiv g_{i1}^{-T} (x_{1im} + \dots + x_{Kim})^T \\
 &\equiv g_{i1}^{-T} (\alpha_i H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \beta_{i1} + \dots + \alpha_i H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}] + \beta_{iK})^T \\
 &\equiv g_{i1}^{-T} (\alpha_i (H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \dots + H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}]) + \lambda \infty)^T \\
 &\equiv g_{i1}^{-T} (\alpha_i (H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \dots + H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}]))^T \\
 &\equiv g_{i1}^{(H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \dots + H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}])^T} \pmod{N}
 \end{aligned}$$

where

g_{tim} (= vector g_{it} [vector I_{m1}]) is a component corresponding to vector I_{m1} for entity m , selected from own vector g_{it} for 1st block

of information specifying entity i ($t = 0, 1, 2, \dots, T$);

$x_{1im} = \text{vector } s_{i1} [\text{vector } I_{m1}]$;

x_{jim} (= vector s_{ij} [vector I_{mj}]) is a component

5 corresponding to vector I_{mj} for entity m ,
selected from own vector s_{ij} for j 'th block
of information specifying entity i ($j = 2, 3, \dots, K$);

K_{im} is a common key generated by one entity i
10 for another entity m ; and

y_{im} is sum of $(K-1)$ components x_{jim} ($j = 2, 3, \dots, K$), that is, $y_{im} = x_{2im} + x_{3im} + \dots$
 $+ x_{Kim}$.

15 19. A common key generator provided at entities in
a cryptographic communications system for generating a
common key to be used in processing to encrypt plaintext
to ciphertext and in processing to decrypt ciphertext
back to plaintext, comprising:

20 storage means for storing secret keys peculiar to
said entities produced, according to computation formulas
given below, for divided specifying information resulting
from division of information specifying each of said
entities into a plurality of blocks;

25 selection means for selecting components
corresponding to divided specifying information for

opposite entities to be communicated with, from the secret keys stored; and

means for generating said common keys, according to computation formulas given below, using said components

5 so selected:

$$\begin{aligned}\vec{S}_{i1} &= \alpha_i H_1 [\vec{I}_{i1}] + \beta_{i1} \vec{1} \\ \vec{S}_{i2} &= \alpha_i H_2 [\vec{I}_{i2}] + \beta_{i2} \vec{1} \\ \vdots \\ \vec{S}_{ij} &= \alpha_i H_j [\vec{I}_{ij}] + \beta_{ij} \vec{1} \\ \vdots \\ \vec{S}_{iK} &= \alpha_i H_K [\vec{I}_{iK}] + \beta_{iK} \vec{1}\end{aligned}$$

10

$$\begin{aligned}\vec{g}_{i0} &\equiv g \alpha_i^{-T} \vec{1} \pmod{N} \\ \vec{g}_{i1} &\equiv g \alpha_i^{-T} \vec{S}_{i1} \pmod{N} \\ \vec{g}_{i2} &\equiv g \alpha_i^{-T} \langle \vec{S}_{i1} \rangle^2 \pmod{N} \\ \vdots \\ \vec{g}_{it} &\equiv g \alpha_i^{-T} \langle \vec{S}_{i1} \rangle^t \pmod{N} \\ \vdots \\ \vec{g}_{iT} &\equiv g \alpha_i^{-T} \langle \vec{S}_{i1} \rangle^T \pmod{N}\end{aligned}$$

15

where

vector s_{ij} is a secret key corresponding to j 'th

divided specifying information for entity

i ($j = 1, 2, \dots, K$)

20

[vector I_{ij}] is j 'th divided specifying

information for entity i ;

vector $\vec{1}$ is a vector of dimension K wherein all

components are 1;

H_j is a symmetrical $2^{M_j} \times 2^{M_j}$ matrix made up of

25

random numbers;

M_j is size of j 'th divided specifying
information for entity i ;

K is number of block divisions in information
specifying entity i ;

5 α_i is a personal secret random number for entity
 i (where $\gcd(\alpha_i, \lambda(N)) = 1$ and $\lambda(\cdot)$ is
Carmichael function);

N is such that $N = PQ$ (where P and Q are
prime);

10 β_{ij} is a personal secret random number for
entity i (where $\beta_{i1} + \beta_{i2} + \dots + \beta_{iK} =$
 $\lambda(N)$);

g is maximum generating element with modulo N ;

vector g_{it} is a secret key for 1st block of
15 information specifying entity i ($t = 0,$
 $1, 2, \dots, T$);

T is degree of exponent portion; and

if c is a scalar, and A and B are matrixes
represented in (i) and (ii) below, the
20 expressions $B = c^A$ and $B = \langle A \rangle^c$ represent
(iii) and (iv) below, respectively.

(i) $A = (a_{\mu\nu})$

25 (ii) $B = (b_{\mu\nu})$

(iii) $b_{\mu\nu} = c^{a_{\mu\nu}}$

(iv) $b_{\mu\nu} = a_{\mu\nu}^c$

$$g_{0im} = \overrightarrow{g_{i0}} [\overrightarrow{I_{m1}}]$$

$$g_{1im} = \overrightarrow{g_{i1}} [\overrightarrow{I_{m1}}]$$

$$\vdots$$

$$g_{tim} = \overrightarrow{g_{it}} [\overrightarrow{I_{m1}}]$$

$$g_{Tim} = \overrightarrow{g_{iT}} [\overrightarrow{I_{m1}}]$$

5

$$x_{2im} = \overrightarrow{s_{i2}} [\overrightarrow{I_{m2}}]$$

$$\vdots$$

$$x_{jim} = \overrightarrow{s_{ij}} [\overrightarrow{I_{mj}}]$$

$$x_{Kim} = \overrightarrow{s_{iK}} [\overrightarrow{I_{mK}}]$$

10

$$\begin{aligned} K_{im} &\equiv \prod_{t=0}^T g_{tim}^{T C_t y_{im}^{(T-t)}} \\ &\equiv g_{i1}^{-T} \sum_{t=0}^T C x_{1im}^t y_{im}^{T-t} \\ &\equiv g_{i1}^{-T} (x_{1im} + y_{im})^T \\ &\equiv g_{i1}^{-T} (x_{1im} + \dots + x_{kim})^T \\ &\equiv g_{i1}^{-T} (\alpha_i H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \beta_{i1} + \dots + \alpha_i H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}] + \beta_{iK})^T \\ &\equiv g_{i1}^{-T} \{ \alpha_i (H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \dots + H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}]) + \lambda \mathbb{N} \}^T \\ &\equiv g_{i1}^{-T} \{ \alpha_i (H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \dots + H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}]) \}^T \\ &\equiv g_{i1}^{-T} (H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \dots + H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}])^T \pmod{N} \end{aligned}$$

15

where

20

g_{tim} (= vector g_{it} [vector I_{m1}]) is a component corresponding to vector I_{m1} for entity m , selected from own vector g_{it} for 1st block of information specifying entity i ($t = 0, 1, 2, \dots, T$);

25

x_{1im} = vector s_{i1} [vector I_{m1}];

x_{jim} (= vector s_{ij} [vector I_{mj}]) is a component

corresponding to vector I_{mj} for entity m ,
selected from own vector s_{ij} for j 'th block
of information specifying entity i ($j = 2$,
3, ..., K);

5 K_{im} is a common key generated by one entity i
for another entity m ; and

y_{im} is sum of $(K-1)$ components x_{jim} ($j = 2, 3$,
..., K), that is, $y_{im} = x_{2im} + x_{3im} + \dots$
+ x_{Kim} .

10

20. A cryptographic communications system for
reciprocally performing, between a plurality of entities,
encryption processing for encrypting plaintext that is
information to be sent into ciphertext and decryption
15 processing for decrypting ciphertext so sent back into
original plaintext, comprising:

a plurality of centers each of which generates
secret keys peculiar to said entities, according to
computation formulas given below, using divided
20 specifying information resulting from division of
information specifying each of said entities into a
plurality of blocks, and sends said secret keys to said
entities; and

a plurality of entities each of which generates a
25 common key mutually employed in said encryption and
decryption processing when communicating with another

entity, according to computation formulas given below,
using a component contained in own secret key sent from
said centers, the component corresponding to divided
specifying information for said another entity:

$$\begin{aligned}
 \vec{S}_{i1} &= \alpha_i H_1[\vec{I}_{i1}] + \beta_{i1} \vec{1} \\
 \vec{S}_{i2} &= \alpha_i H_2[\vec{I}_{i2}] + \beta_{i2} \vec{1} \\
 &\vdots \\
 \vec{S}_{ij} &= \alpha_i H_j[\vec{I}_{ij}] + \beta_{ij} \vec{1} \\
 &\vdots \\
 \vec{S}_{iK} &= \alpha_i H_K[\vec{I}_{iK}] + \beta_{iK} \vec{1} \\
 \\
 \vec{g}_{i0} &\equiv g^{\alpha_i^{-T}} \vec{1} \pmod{N} \\
 \vec{g}_{i1} &\equiv g^{\alpha_i^{-T}} \vec{S}_{i1} \pmod{N} \\
 \vec{g}_{i2} &\equiv g^{\alpha_i^{-T}} \langle \vec{S}_{i1} \rangle^2 \pmod{N} \\
 &\vdots \\
 \vec{g}_{it} &\equiv g^{\alpha_i^{-T}} \langle \vec{S}_{i1} \rangle^t \pmod{N} \\
 &\vdots \\
 \vec{g}_{iT} &\equiv g^{\alpha_i^{-T}} \langle \vec{S}_{i1} \rangle^T \pmod{N}
 \end{aligned}$$

where

- 15 vector s_{ij} is a secret key corresponding to j 'th
divided specifying information for entity
 i ($j = 1, 2, \dots, K$)
[vector I_{ij}] is j 'th divided specifying
information for entity i ;
- 20 vector 1 is a vector of dimension K wherein all
components are 1 ;
- H_j is a symmetrical $2^{M_j} \times 2^{M_j}$ matrix made up of
random numbers;
- M_j is size of j 'th divided specifying
25 information for entity i ;

K is number of block divisions in information
specifying entity i;

α_i is a personal secret random number for entity
i (where $\gcd(\alpha_i, \lambda(N)) = 1$ and $\lambda(\cdot)$ is
Carmichael function);

N is such that $N = PQ$ (where P and Q are
prime);

β_{ij} is a personal secret random number for
entity i (where $\beta_{i1} + \beta_{i2} + \dots + \beta_{iK} =$
 $\lambda(N)$);

g is maximum generating element with modulo N;
vector g_{it} is a secret key for 1st block of
information specifying entity i ($t = 0,$
 $1, 2, \dots, T$);

T is degree of exponent portion; and
if c is a scalar, and A and B are matrixes
represented in (i) and (ii) below, the
expressions $B = c^A$ and $B = \langle A \rangle^c$ represent
(iii) and (iv) below, respectively.

(i) $A = (a_{\mu\nu})$

(ii) $B = (b_{\mu\nu})$

(iii) $b_{\mu\nu} = c^{a_{\mu\nu}}$

(iv) $b_{\mu\nu} = a_{\mu\nu}^c$

$g_{0im} = \overrightarrow{g_{i0}} [\overrightarrow{I_{m1}}]$

$$\begin{aligned}
\vec{g}_{1im} &= \vec{g}_{i1} [\vec{I}_{m1}] \\
\vdots \\
\vec{g}_{tim} &= \vec{g}_{it} [\vec{I}_{m1}] \\
\vdots \\
\vec{g}_{Tim} &= \vec{g}_{iT} [\vec{I}_{m1}] \\
\vec{x}_{2im} &= \vec{s}_{i2} [\vec{I}_{m2}] \\
\vdots \\
\vec{x}_{jim} &= \vec{s}_{ij} [\vec{I}_{mj}] \\
\vdots \\
\vec{x}_{Kim} &= \vec{s}_{iK} [\vec{I}_{mK}]
\end{aligned}$$

5

$$\begin{aligned}
K_{im} &\equiv \prod_{t=0}^T \vec{g}_{tim}^{T C_t y_{im}^{(T-t)}} \\
&\equiv \vec{g}_i^{-T} \sum_{t=0}^T C_{1im}^t y_{im}^{T-t} \\
&\equiv \vec{g}_i^{-T} (x_{1im} + y_{im})^T \\
&\equiv \vec{g}_i^{-T} (x_{1im} + \dots + x_{kim})^T \\
&\equiv \vec{g}_i^{-T} (\alpha_i H_1 [\vec{I}_{i1}] [\vec{I}_{m1}] + \beta_{i1} + \dots + \alpha_i H_K [\vec{I}_{iK}] [\vec{I}_{mK}] + \beta_{iK})^T \\
&\equiv \vec{g}_i^{-T} (\alpha_i (H_1 [\vec{I}_{i1}] [\vec{I}_{m1}] + \dots + H_K [\vec{I}_{iK}] [\vec{I}_{mK}]) + \lambda (N))^T \\
&\equiv \vec{g}_i^{-T} (\alpha_i (H_1 [\vec{I}_{i1}] [\vec{I}_{m1}] + \dots + H_K [\vec{I}_{iK}] [\vec{I}_{mK}]))^T \\
&\equiv \vec{g}_i^{-T} (H_1 [\vec{I}_{i1}] [\vec{I}_{m1}] + \dots + H_K [\vec{I}_{iK}] [\vec{I}_{mK}])^T \pmod{N}
\end{aligned}$$

10

15

where

\vec{g}_{tim} (= vector \vec{g}_{it} [vector \vec{I}_{m1}]) is a component corresponding to vector \vec{I}_{m1} for entity m , selected from own vector \vec{g}_{it} for 1st block of information specifying entity i ($t = 0, 1, 2, \dots, T$);

\vec{x}_{1im} = vector \vec{s}_{i1} [vector \vec{I}_{m1}];

\vec{x}_{jim} (= vector \vec{s}_{ij} [vector \vec{I}_{mj}]) is a component corresponding to vector \vec{I}_{mj} for entity m , selected from own vector \vec{s}_{ij} for j 'th block

20

25

of information specifying entity i ($j = 2, 3, \dots, K$);

K_{im} is a common key generated by one entity i for another entity m ; and

5 y_{im} is sum of $(K-1)$ components x_{jim} ($j = 2, 3, \dots, K$), that is, $y_{im} = x_{2im} + x_{3im} + \dots + x_{Kim}$.

21. A computer readable recording medium for
10 storing a program that generates at entities involved in communications a common key mutually used in processing to encrypt plaintext to ciphertext and in processing to decrypt said ciphertext back to said plaintext in a cryptographic communications system, comprising:

15 first program code means for causing said computer to select a component corresponding to divided specifying information of one entity that is a ciphertext recipient from a secret key peculiar to another entity that is a ciphertext sender, according to computation formulas
20 given below, for each of divided specifying information resulting from division of information specifying each of said entities into a plurality of blocks; and

second program code means for causing said computer to generate said common key, according to computation
25 formulas given below, using said components selected:

$$\overrightarrow{S_{i1}} = \alpha_{i1} H_1[\overrightarrow{I_{i1}}] + \beta_{i1} \overrightarrow{1}$$

$$\vec{S}_{i2} = \alpha_i H_2 [\vec{I}_{i2}] + \beta_{i2} \vec{1}$$

$$\vec{S}_{ij} = \alpha_i H_j [\vec{I}_{ij}] + \beta_{ij} \vec{1}$$

$$\vec{S}_{iK} = \alpha_i H_K [\vec{I}_{iK}] + \beta_{iK} \vec{1}$$

$$\vec{g}_{i0} \equiv g \alpha_i^{-T} \vec{1} \pmod{N}$$

$$5 \quad \vec{g}_{i1} \equiv g \alpha_i^{-T} \vec{S}_{i1} \pmod{N}$$

$$\vec{g}_{i2} \equiv g \alpha_i^{-T} \langle \vec{S}_{i1} \rangle^2 \pmod{N}$$

$$\vec{g}_{it} \equiv g \alpha_i^{-T} \langle \vec{S}_{i1} \rangle^t \pmod{N}$$

$$\vec{g}_{iT} \equiv g \alpha_i^{-T} \langle \vec{S}_{i1} \rangle^T \pmod{N}$$

10 where

vector s_{ij} is a secret key corresponding to j 'th

divided specifying information for entity

i ($j = 1, 2, \dots, K$)

[vector I_{ij}] is j 'th divided specifying

15 information for entity i ;

vector 1 is a vector of dimension K wherein all

components are 1 ;

H_j is a symmetrical $2^{M_j} \times 2^{M_j}$ matrix made up of

random numbers;

20 M_j is size of j 'th divided specifying

information for entity i ;

K is number of block divisions in information

specifying entity i ;

α_i is a personal secret random number for entity

25 i (where $\gcd(\alpha_i, \lambda(N)) = 1$ and $\lambda(\cdot)$ is

Carmichael function);

N is such that $N = PQ$ (where P and Q are
prime);

β_{ij} is a personal secret random number for
5 entity i (where $\beta_{i1} + \beta_{i2} + \dots + \beta_{iK} =$
 $\lambda(N)$);

g is maximum generating element with modulo N;
vector g_{it} is a secret key for 1st block of

information specifying entity i ($t = 0,$
10 $1, 2, \dots, T$);

T is degree of exponent portion; and

if c is a scalar, and A and B are matrixes
represented in (i) and (ii) below, the
expressions $B = c^A$ and $B = \langle A \rangle^c$ represent
15 (iii) and (iv) below, respectively.

(i) $A = (a_{\mu\nu})$

(ii) $B = (b_{\mu\nu})$

(iii) $b_{\mu\nu} = c^{a_{\mu\nu}}$

(iv) $b_{\mu\nu} = a_{\mu\nu}^c$

25 $g_{0im} = \overrightarrow{g_{i0}} [\overrightarrow{I_{m1}}]$

$g_{1im} = \overrightarrow{g_{i1}} [\overrightarrow{I_{m1}}]$

\vdots
 $g_{tim} = \overrightarrow{g_{it}} [\overrightarrow{I_{m1}}]$

\vdots
 $g_{Tim} = \overrightarrow{g_{iT}} [\overrightarrow{I_{m1}}]$

$$\begin{aligned} x_{2im} &= s_{i2} [\vec{I}_{m2}] \\ x_{jim} &= s_{ij} [\vec{I}_{mj}] \\ x_{kim} &= s_{iK} [\vec{I}_{mK}] \end{aligned}$$

$$\begin{aligned} 5 \quad K_{im} &\equiv \prod_{t=0}^T g_{tim}^{C_t y_{im}^{(T-t)}} \\ &\equiv g_i^{-T} \sum_{t=0}^T C_{x_{lim}}^t y_{im}^{T-t} \\ &\equiv g_i^{-T} (x_{lim} + y_{im})^T \\ &\equiv g_i^{-T} (x_{lim} + \dots + x_{kim})^T \\ &\equiv g_i^{-T} (\alpha_1 H_1 [\vec{I}_{i1}] [\vec{I}_{m1}] + \beta_1 + \dots + \alpha_K H_K [\vec{I}_{iK}] [\vec{I}_{mK}] + \beta_K)^T \\ &\equiv g_i^{-T} \{ \alpha_i (H_1 [\vec{I}_{i1}] [\vec{I}_{m1}] + \dots + H_K [\vec{I}_{iK}] [\vec{I}_{mK}]) + \lambda \emptyset \}^T \\ 10 \quad &\equiv g_i^{-T} \{ \alpha_i (H_1 [\vec{I}_{i1}] [\vec{I}_{m1}] + \dots + H_K [\vec{I}_{iK}] [\vec{I}_{mK}]) \}^T \\ &\equiv g_i^{-T} (H_1 [\vec{I}_{i1}] [\vec{I}_{m1}] + \dots + H_K [\vec{I}_{iK}] [\vec{I}_{mK}])^T \pmod{N} \end{aligned}$$

where

g_{tim} (= vector g_{it} [vector I_{m1}]) is a component corresponding to vector I_{m1} for entity m , selected from own vector g_{it} for 1st block of information specifying entity i ($t = 0, 1, 2, \dots, T$);

x_{lim} = vector s_{i1} [vector I_{m1}];

x_{jim} (= vector s_{ij} [vector I_{mj}]) is a component

corresponding to vector I_{mj} for entity m , selected from own vector s_{ij} for j 'th block of information specifying entity i ($j = 2, 3, \dots, K$);

K_{im} is a common key generated by one entity i for another entity m ; and

y_{im} is sum of $(K-1)$ components x_{jim} ($j = 2, 3,$

..., K), that is, $y_{im} = x_{2im} + x_{3im} + \dots$
 $+ x_{kim}$.

22. A computer data signal embodied in a carrier
5 wave for generating at entities involved in
communications common keys used in processing to encrypt
plaintext to ciphertext and in processing to decrypt said
ciphertext to said plaintext in a cryptographic
communications system, comprising:

10 first code segment for causing a computer to select
a component corresponding to one or more of divided
pieces of information specifying one entity from a secret
key peculiar to another entity; and

second code segment for causing said computer to
15 generate said common keys using said components selected.

23. A computer data signal embodied in a carrier
wave for generating at entities involved in
communications a common key mutually used in processing
20 to encrypt plaintext to ciphertext and in processing to
decrypt said ciphertext back to said plaintext in a
cryptographic communications system, comprising:

first code segment for causing a computer to select
a component corresponding to divided specifying
25 information of one entity that is a ciphertext recipient
from a secret key peculiar to another entity that is a

ciphertext sender, according to computation formulas given below, for each of divided specifying information resulting from division of information specifying each of said entities into a plurality of blocks; and

5 second code segment for causing said computer to generate said common key, according to computation formulas given below, using said components selected:

$$\begin{aligned}
 \vec{S}_{i1} &= \alpha_i H_1 [\vec{I}_{i1}] + \beta_{i1} \vec{1} \\
 \vec{S}_{i2} &= \alpha_i H_2 [\vec{I}_{i2}] + \beta_{i2} \vec{1} \\
 \vec{S}_{ij} &= \alpha_i H_j [\vec{I}_{ij}] + \beta_{ij} \vec{1} \\
 \vec{S}_{iK} &= \alpha_i H_K [\vec{I}_{iK}] + \beta_{iK} \vec{1} \\
 \\
 \vec{g}_{i0} &\equiv g \alpha_i^{-T} \vec{1} \pmod{N} \\
 \vec{g}_{i1} &\equiv g \alpha_i^{-T} \vec{S}_{i1} \pmod{N} \\
 \vec{g}_{i2} &\equiv g \alpha_i^{-T} \langle \vec{S}_{i1} \rangle^2 \pmod{N} \\
 \vec{g}_{it} &\equiv g \alpha_i^{-T} \langle \vec{S}_{i1} \rangle^t \pmod{N} \\
 \vec{g}_{iT} &\equiv g \alpha_i^{-T} \langle \vec{S}_{i1} \rangle^T \pmod{N}
 \end{aligned}$$

where

vector s_{ij} is a secret key corresponding to j 'th
 20 divided specifying information for entity
 i ($j = 1, 2, \dots, K$)
 $[\text{vector } I_{ij}]$ is j 'th divided specifying
 information for entity i ;
 vector 1 is a vector of dimension K wherein all
 25 components are 1;

H_j is a symmetrical $2^{M_j} \times 2^{M_j}$ matrix made up of random numbers;

M_j is size of j 'th divided specifying information for entity i ;

5 K is number of block divisions in information specifying entity i ;

α_i is a personal secret random number for entity i (where $\gcd(\alpha_i, \lambda(N)) = 1$ and $\lambda(\cdot)$ is Carmichael function);

10 N is such that $N = PQ$ (where P and Q are prime);

β_{ij} is a personal secret random number for entity i (where $\beta_{i1} + \beta_{i2} + \dots + \beta_{iK} = \lambda(N)$);

15 g is maximum generating element with modulo N ;
vector g_{it} is a secret key for 1st block of information specifying entity i ($t = 0, 1, 2, \dots, T$);

T is degree of exponent portion; and

20 if c is a scalar, and A and B are matrixes represented in (i) and (ii) below, the expressions $B = c^A$ and $B = \langle A \rangle^c$ represent (iii) and (iv) below, respectively.

25 (i) $A = (a_{\mu\nu})$

$$(ii) \quad B = (b_{\mu\nu})$$

$$(iii) \quad b_{\mu\nu} = c^{a_{\mu\nu}}$$

$$5 \quad (iv) \quad b_{\mu\nu} = a_{\mu\nu}^c$$

$$g_{0im} = \overrightarrow{g_{i0}} [\overrightarrow{I_{m1}}]$$

$$g_{1im} = \overrightarrow{g_{i1}} [\overrightarrow{I_{m1}}]$$

$$10 \quad g_{tim} = \overrightarrow{g_{it}} [\overrightarrow{I_{m1}}]$$

$$g_{Tim} = \overrightarrow{g_{iT}} [\overrightarrow{I_{m1}}]$$

$$x_{2im} = \overrightarrow{s_{i2}} [\overrightarrow{I_{m2}}]$$

$$x_{jim} = \overrightarrow{s_{ij}} [\overrightarrow{I_{mj}}]$$

$$x_{Kim} = \overrightarrow{s_{iK}} [\overrightarrow{I_{mK}}]$$

15

$$\begin{aligned} K_{im} &\equiv \prod_{t=0}^T g_{tim}^{T C_t y_{im}^{(T-t)}} \\ &\equiv g_{i1}^{-T} \sum_{t=0}^T C_{1im}^t y_{im}^{T-t} \\ &\equiv g_{i1}^{-T} (x_{1im} + y_{im})^T \\ &\equiv g_{i1}^{-T} (x_{1im} + \dots + x_{kim})^T \\ &\equiv g_{i1}^{-T} (\alpha_{i1} \overrightarrow{H_1} [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \beta_{i1} + \dots + \alpha_{iK} \overrightarrow{H_K} [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}] + \beta_{iK})^T \\ 20 \quad &\equiv g_{i1}^{-T} (\alpha_i (\overrightarrow{H_1} [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \dots + \overrightarrow{H_K} [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}]) + \lambda \mathbb{O})^T \\ &\equiv g_{i1}^{-T} (\alpha_i (\overrightarrow{H_1} [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \dots + \overrightarrow{H_K} [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}]))^T \\ &\equiv g_{i1}^{-T} (\overrightarrow{H_1} [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \dots + \overrightarrow{H_K} [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}])^T \pmod{N} \end{aligned}$$

20

where

25

g_{tim} (= vector g_{it} [vector I_{m1}]) is a component corresponding to vector I_{m1} for entity m , selected from own vector g_{it} for 1st block of information specifying entity i ($t = 0, 1, 2, \dots, T$);

$x_{1im} = \text{vector } s_{i1} [\text{vector } I_{m1}];$

x_{jim} (= vector s_{ij} [vector I_{mj}]) is a component
corresponding to vector I_{mj} for entity m ,
selected from own vector s_{ij} for j 'th block
of information specifying entity i ($j = 2,$
3, ..., K);

K_{im} is a common key generated by one entity i
for another entity m ; and

y_{im} is sum of $(K-1)$ components x_{jim} ($j = 2, 3,$
..., K), that is, $y_{im} = x_{2im} + x_{3im} + \dots$

+ x_{Kim} .

ABSTRACT OF THE DISCLOSURE

A cryptographic communications method based on ID-NIKS, wherewith mathematical structures are minimized, 5 the collusion problem can be circumvented, and building the cryptosystem is simplified. A plurality of centers are provided for distributing a plurality of secret keys to a plurality of entities, respectively. Each secret key is unique to each entity. Information specifying the 10 entities (entity ID information) is divided into a plurality of pieces or segments. All secret keys produced for the pieces of entity ID information are distributed to the entities. Using a component contained in the secret key peculiar to itself, each entity generates a 15 common key to be shared by another entity. This component corresponds to a piece of ID information of another entity.

FIG. 1

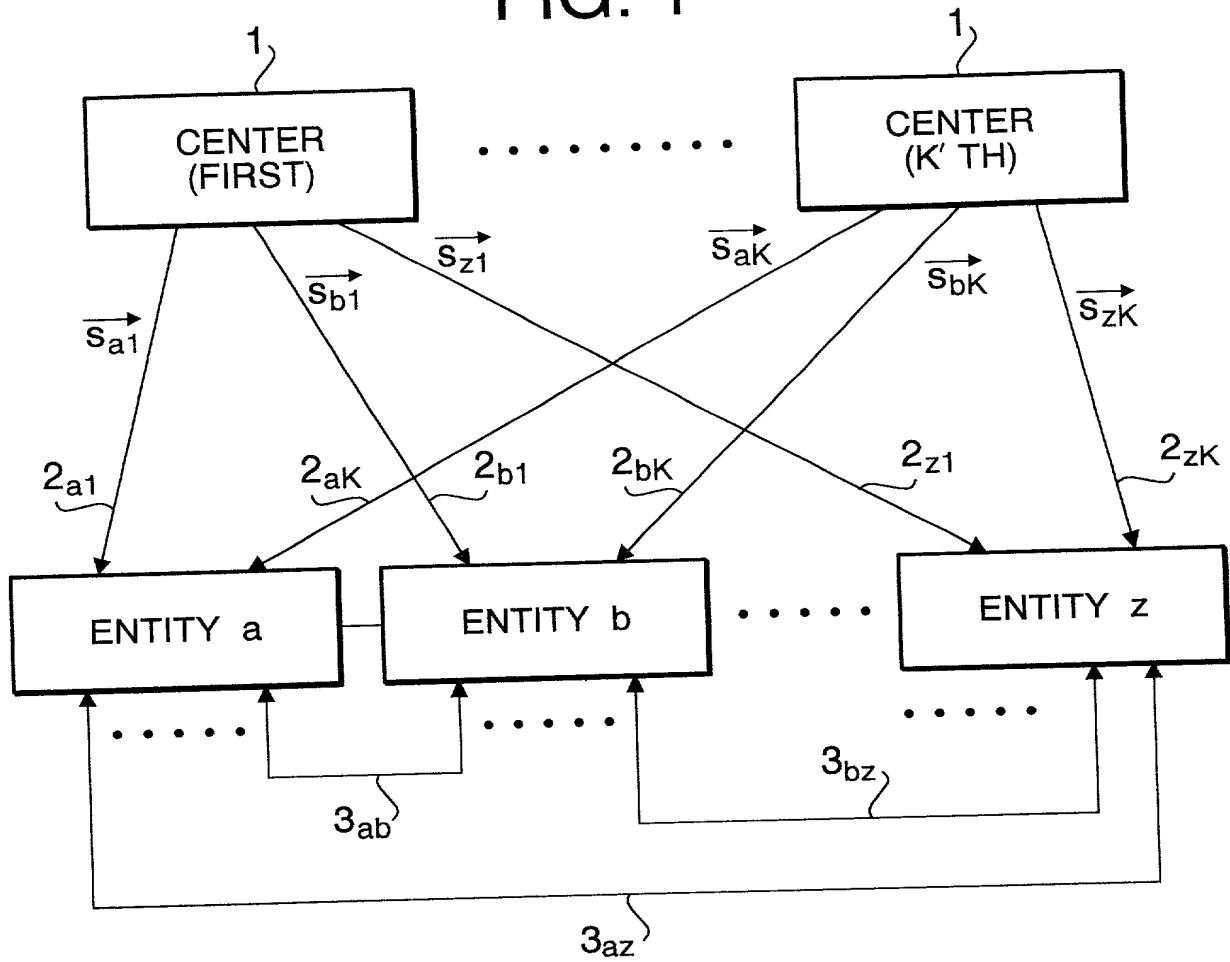
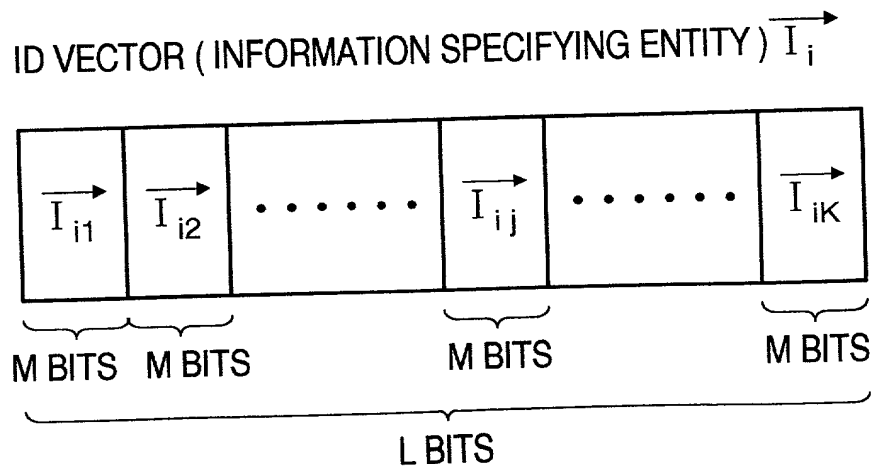


FIG. 2



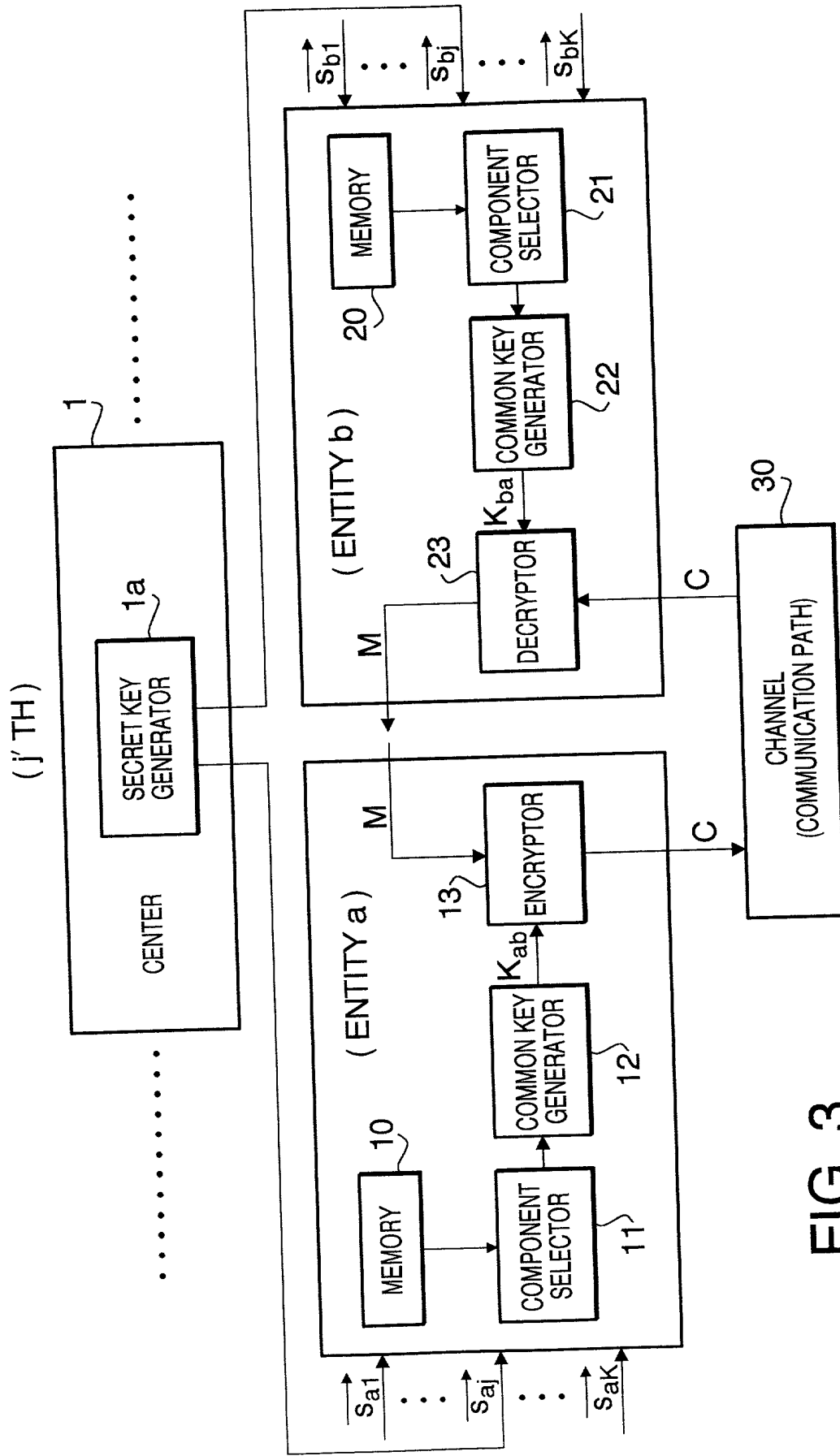


FIG. 3

FIG. 4

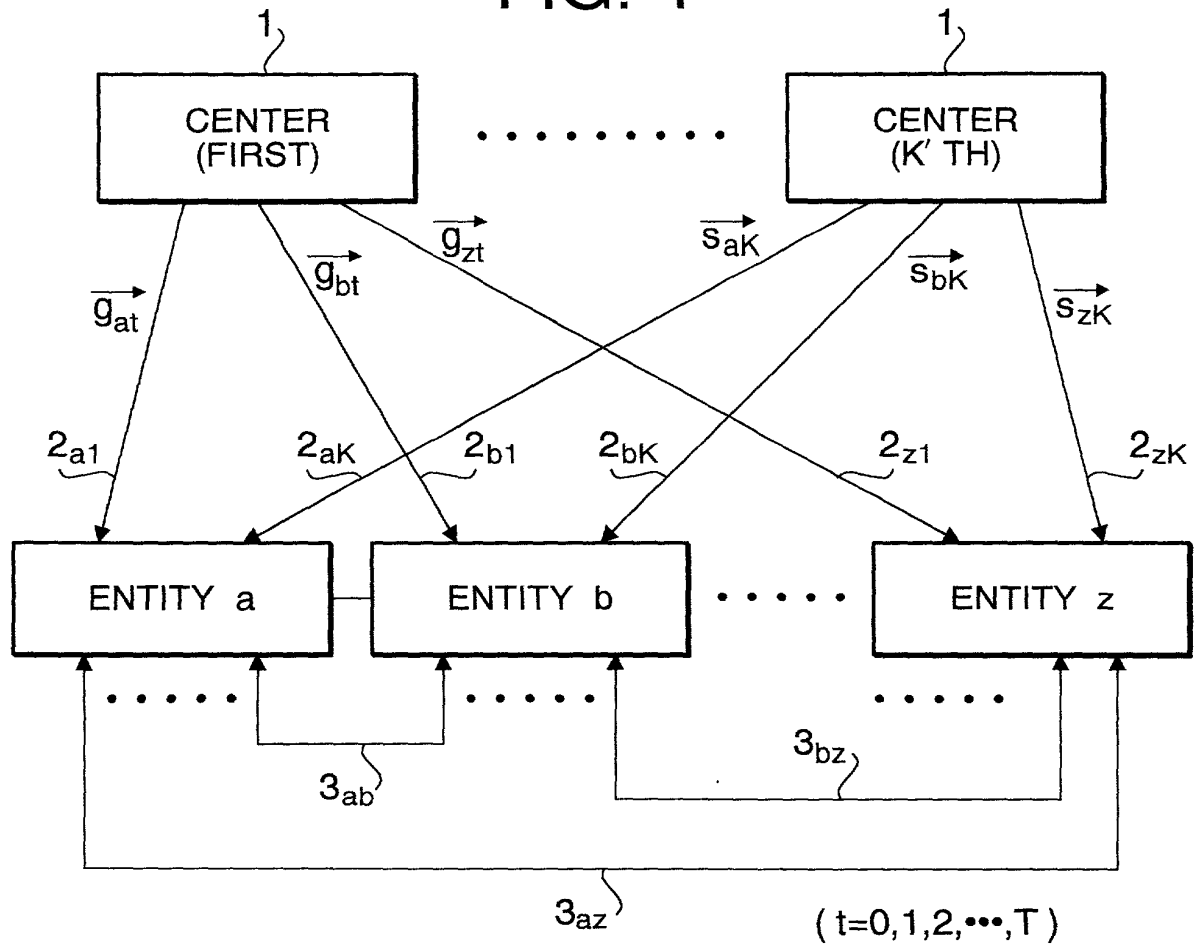
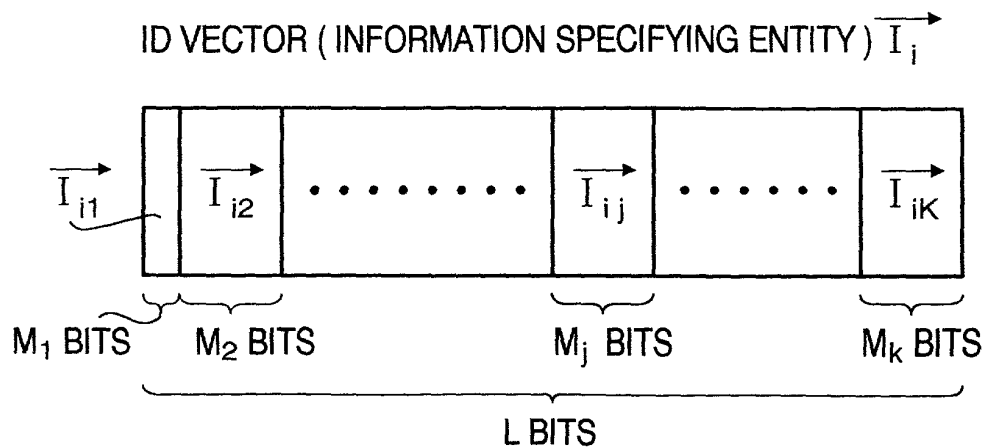


FIG. 5



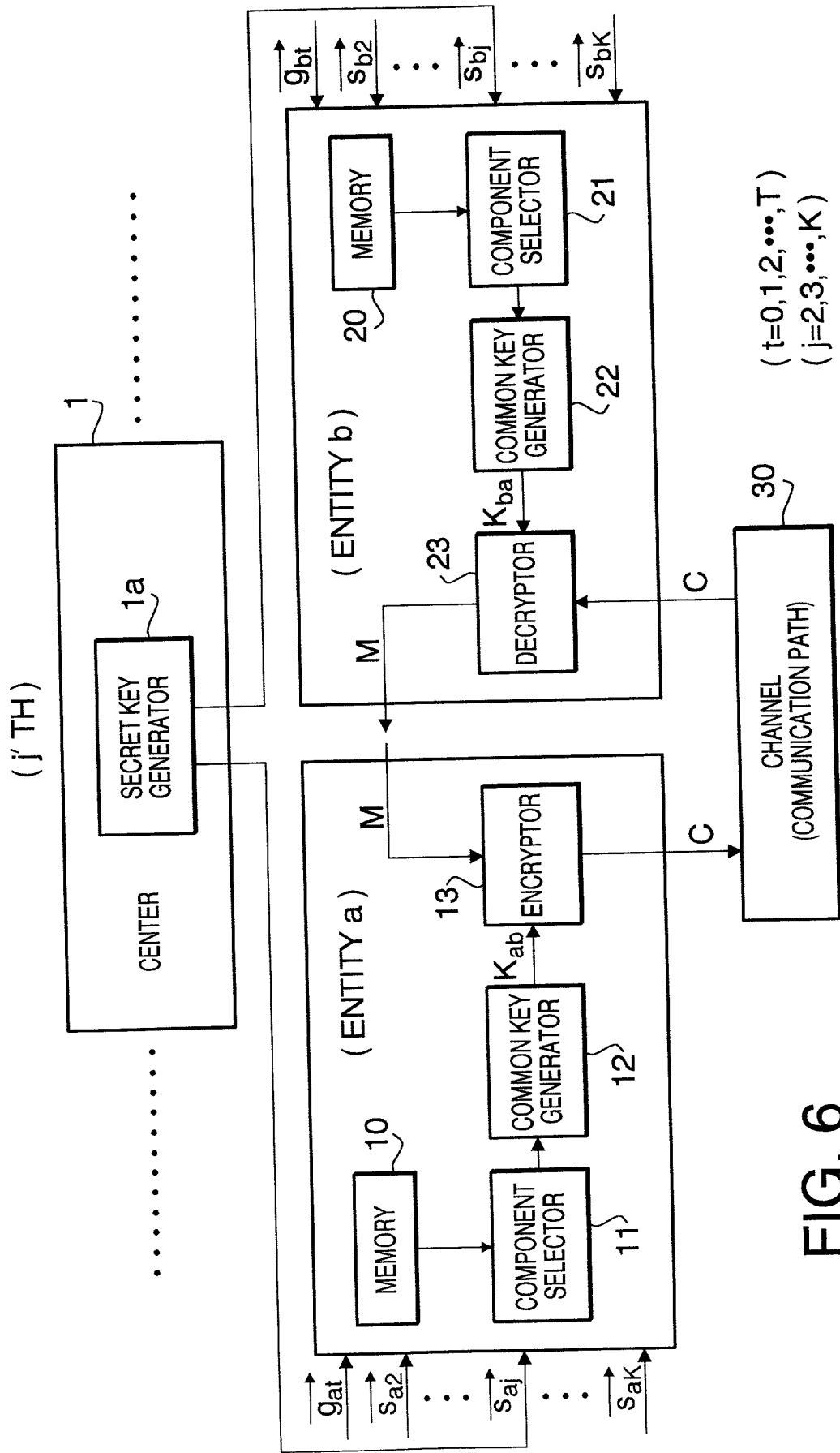
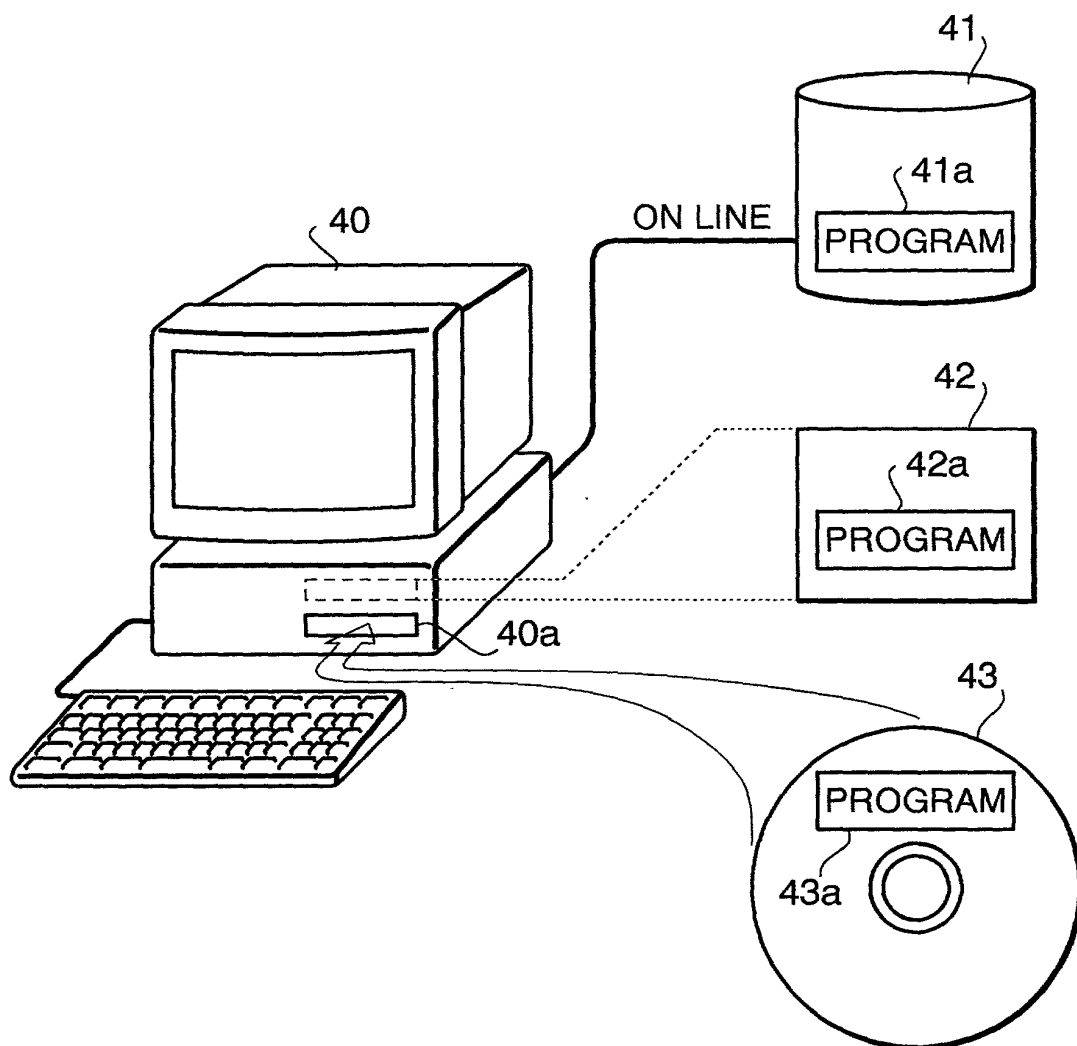


FIG. 6

FIG. 7



DECLARATION
and POWER OF ATTORNEY

KM-US-147

☒ ORIGINAL
☐ CONTINUATION
☐ DIVISIONAL

As a below named inventor, I declare that the information given herein is true, that I believe that I am the original, first and sole inventor (if only one name is listed as 1 below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: **SECRET KEY GENERATION METHOD, ENCRYPTION METHOD, CRYPTOGRAPHIC COMMUNICATIONS METHOD, COMMON KEY GENERATOR, CRYPTOGRAPHIC COMMUNICATIONS SYSTEM, AND RECORDING MEDIA**, the specification of which is attached hereto unless the following box is checked: ☐ was filed on _____ as United States Application Number or PCT International Application Number _____ and was amended on _____

My residence, post office address and citizenship are as stated below next to my name.

I acknowledge my duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations § 1.56(a). I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above. I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

COUNTRY	APPLICATION NUMBER	DATE OF FILING Month Day Year	PRIORITY CLAIMED UNDER 35 U.S.C. 119
Japan	11-16257	January 25, 1999	Yes
Japan	11-59049	March 5, 1999	Yes

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code § 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application.

(Application Serial No.)

(Filing Date)

(Status)

POWER OF ATTORNEY: As a named Inventor, I hereby appoint the following attorney(s) and/or Agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

STUART LUBITZ, Reg. No. 20,680; LOUIS A. MOK, Reg. No. 22,585; JOHN P. SCHERLACHER, Reg. No. 23,009; MICHAEL J. RAM, Reg. No. 26,379; LEWIS ANTEN, Reg. No. 26,604; HIDEO KODA, Reg. No. 27,729; JOANNE S. REDMANN, Reg. No. 31,482; SONG K. JUNG, Reg. No. 35,210; WILLIAM H. WRIGHT, Reg. No. 36,312; AMEDEO FERRARO, Reg. No. 37,129; LEE J. MANDELL, Reg. No. 37,176; JONATHAN Y. KANG, Reg. No. 38,199; DAVID L. LUBITZ, Reg. No. 38,229; WEI-NING YANG, Reg. No. 38,690; KARLTON BUTTS, Reg. No. 39,126; BONITA L. SEVERY, Reg. No. 43,913

Send correspondence to: LOEB & LOEB LLP

DIRECT TELEPHONE CALLS TO:

William H. Wright

10100 Santa Monica Blvd.
Los Angeles, CA 90067-4164

310-282-2000

(Please Print)

1	Name of Inventor	Shigeo Tsujii	Residence: CITY	Shibuya-ku	STATE or COUNTRY	Tokyo, Japan
	Post Office Address	4-2-19, Jingumae, Shibuya-ku, Tokyo			CITIZENSHIP	Japan
2	Name of Inventor	Yasuyuki Murakami	Residence: CITY	Uji-shi	STATE or COUNTRY	Kyoto, Japan
	Post Office Address	Murata Kikai Shataku B-602, 51-6, Makishima-cho Motoyashiki, Uji-shi, Kyoto			CITIZENSHIP	Japan
3	Name of Inventor	Masao Kasahara	Residence: CITY	Minoo-shi	STATE or COUNTRY	Osaka, Japan
	Post Office Address	15-3, Aogeiin 4-chome, Minoo-shi, Osaka			CITIZENSHIP	Japan
4	Name of Inventor		Residence: CITY		STATE or COUNTRY	
	Post Office Address				CITIZENSHIP	

I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

SIGNATURE OF INVENTOR 1	SIGNATURE OF INVENTOR 2
<i>Shigeo Tsujii</i>	<i>Yasuyuki Murakami</i>
DATE January 12, 2000	DATE January 12, 2000
SIGNATURE OF INVENTOR 3	SIGNATURE OF INVENTOR 4
<i>Masao Kasahara</i>	
DATE January 12, 2000	DATE